June 29, 2018

Chairman Greg Walden
Ranking Member Frank Pallone
Energy and Commerce Committee
U.S. House of Representatives
2125 Rayburn House Office Building
Washington, D.C. 20510

Dear Chairman Walden, Ranking Member Pallone, and Members of the Committee:

Thank you for your questions for the record from the April 11, 2018 Hearing titled Facebook: Transparency and Use of Consumer Data. Per your request, attached are the answers for the record for your questions.

Please note that we received over 2,000 questions from the Senate and House Committees before which we testified on April 10 and 11, 2018. We appreciate the time you gave us to respond to these questions. We did our best to review and answer them in the available timeframe. We respectfully request an opportunity to supplement or amend our responses if needed.

Sincerely,

Facebook, Inc.

Address: 1601 Willow Road
Menlo Park, CA 94025

House Energy and Commerce Questions for the Record

The Honorable Greg Walden

1. Restricting outside parties' access to Facebook data was a major topic of discussion at the Energy and Commerce Committee hearing. What additional data and information, from Facebook users or from other third-party companies about Facebook users, does the company collect?

a. Please provide a complete accounting of every data element collected on Facebook users, non-users, and from third-party companies.

b. Are there data elements collected beyond what is necessary to operate the social network platform? If yes, please identify each data element.

As explained in our Data Policy, we collect three basic categories of data about people:

(1) data about things people do and share (and who they connect with) on our services;

(2) data about the devices people use to access our services; and

(3) data we receive from partners, including the websites and apps that use our business tools.

As far as the amount of data we collect about people, the answer depends on the person. People who have only recently signed up for Facebook have usually shared only a few things—such as name, contact information, age, and gender. Over time, as people use our products, we receive more data from them, and this data helps us provide more relevant content and services. That data will fall into the categories noted above, but the specific data we receive will, in large part, depend on how the person chooses to use Facebook. For example, some people use Facebook to share photos, so we receive and store photos for those people. Some people enjoy watching videos on Facebook; when they do, we receive information about the video they watched, and we can use that information to help show other videos in their News Feeds. Other people seldom or never watch videos, so we do not receive the same kind of information from them, and their News Feeds are likely to feature fewer videos.

The data we have about people also depends on how they have used our controls. For example, people who share photos can easily delete those photos. The same is true of any other kind of content that people post on our services. Through Facebook's Activity Log tool, people can also control the information about their engagement—i.e., their likes, shares and comments—with other people's posts. The use of these controls of course affects the data we have about people.

When people visit apps or websites that feature our technologies—like the Facebook Like or Comment button—our servers automatically log (i) standard browser or app records of the fact that a particular device or user visited the website or app (this connection to Facebook's servers occurs automatically when a person visits a website or app that contains our

technologies, such as a Like button, and is an inherent function of internet design); and (ii) any additional information the publisher of the app or website chooses to share with Facebook about the person's activities on that site (such as the fact that a purchase was made on the site). This is a standard feature of the internet, and most websites and apps share this same information with multiple different third-parties whenever people visit their website or app. For example, the House Energy and Commerce Committee's website shares information with Google Analytics to help improve the site. This means that, when a person visits the Committee's website, it sends browser information about their visit to that third party. More information about how this works is available at https://newsroom.fb.com/news/2018/04/data-off-facebook/.

When the person visiting a website featuring Facebook's tools is not a registered Facebook user, Facebook does not have information identifying that individual, and it does not create profiles for this individual.

We use the browser and app logs that apps and websites send to us—described above—in the following ways for non-Facebook users. First, these logs are critical to protecting the security of Facebook and to detecting or preventing fake account access. For example, if a browser has visited hundreds of sites in the last five minutes, that's a sign the device might be a bot, which would be an important signal of a potentially inauthentic account if that browser then attempted to register for an account. Second, we aggregate those logs to provide summaries and insights to websites and apps about how many people visit or use their product, or use specific features like our Like button—but without providing any information about a specific person. We do not create profiles for non-Facebook users, nor do we use browser and app logs for non-Facebook users to show targeted ads from our advertisers to them or otherwise seek to personalize the content they see. However, we may take the opportunity to show a general ad that is unrelated to the attributes of the person or an ad encouraging the non-user to sign up for Facebook.

We do receive some information from devices and browsers that may be used by non-users. For example:

- We also may receive information about the device of a non-registered user if that user visits a part of Facebook that does not require people to log in—such as a public Facebook Page. The information we log when people visit our websites or apps is the same as described above and is the same information that any provider of an online service would receive.

- In addition, Facebook may receive some basic information about devices where Facebook apps are installed, including before people using those devices have registered for Facebook (such as when a user downloads a Facebook app, but has not yet created an account, or if the app is preloaded on a given device). This device data includes things like device model, operating system, IP address, app version and device identifiers. We use this information to provide the right version of the app, help people who want to create accounts (for example, optimizing the registration flow for the specific device), retrieving bug fixes and measuring and improving app performance. We do not use this information to build profiles about non-registered users.

2. At the April 11 hearing, it was revealed that Facebook's 2 billion users likely had their public profiles scraped (meaning information about individuals, accessible to third party apps on the Facebook Platform, was easily pulled off the service, typically in large quantities, and made accessible to others outside the platform) by outsiders—third-party developers.

a. How long have third-parties been able to scrape data from Facebook users and their friends' pages? The testimony indicated the mechanisms used by Cambridge Analytica, Obama for America, and countless other third-party applications were no longer available after 2014. Please detail what information third-party applications can remove from Facebook about users and their friends as of January 2018 and, separately, today, if there is any difference.

We understand your question to be about updates to our app platform. In 2007, there was industry-wide interest in enriching and expanding users' experiences on various platforms by allowing them to take their data (from a device or service) to third-party developers to receive new experiences. For example, around that time, Apple and Google respectively launched their iOS and Android platforms, which were quickly followed by platform technologies and APIs that allowed developers to develop applications for those two platforms and distribute them to users through a variety of channels. Similarly, in 2007, Facebook launched a set of platform technologies that allowed third parties to build applications that could run on and integrate with the Facebook service and that could be installed by Facebook users who chose to do so. In December 2009, Facebook launched new privacy controls that enabled users to control which of the types of information that they made available to their friends could be accessed by apps used by those friends.

As with all of these platforms, the permissions model that governed the information that third-party applications could access from the Platform evolved. For example, in April 2010, Facebook launched granular data permissions (GDP), which allowed users to examine a list of categories of information that an app sought permission to access before they authorized the app.

In November 2013, when Kogan launched the app, apps generally could be launched on the Platform without affirmative review or approval by Facebook. The app used the Facebook Login service, which allowed users to utilize their Facebook credentials to authenticate themselves to third-party services. Facebook Login and Facebook's Graph API also allowed the app to request permission from its users to bring their Facebook data (their own data and data shared with them by their friends) to the app, to obtain new experiences.

At that time, the Graph API V1 allowed app developers to request consent to access information from the installing user such as name, gender, birthdate, location (i.e., current city or hometown), photos and Page likes—and also (depending on, and in accordance with, each friend's own privacy settings) the same or similar categories of information the user's friends had shared with the installing user. Permitting users to share data made available to them by their friends had the upside of making the experience of app users more personalized and social. For example, a Facebook user might want to use a music app that allowed the user to (1) see what his or her friends were listening to and (2) give the app permission to access the user's friend list and

thereby know which of the user's friends were also using the app. Such access to information about an app user's friends required not only the consent of the app user, but also required that the friends whose data would be accessed have their own privacy settings set to permit such access by third-party apps. In other words, Kogan's app could have accessed a user's friends' information only for friends whose privacy settings permitted such sharing.

In April 2014, we announced that we would more tightly restrict our platform APIs to prevent abuse. At that time, we made clear that existing apps would have a year to transition—at which point they would be forced (1) to migrate to the more restricted API and (2) be subject to Facebook's new review and approval protocols. The vast majority of companies were required to make the changes by May 2015; a small number of companies (fewer than 100) were given a one-time extension of less than six months beyond May 2015 to come into compliance. (One company received an extension to January 2016.) In addition, in the context of our ongoing review of third-party apps, we discovered a very small number of companies (fewer than 10) that theoretically could have accessed limited friends' data as a result of API access that they received in the context of a beta test. We are not aware that any of this handful of companies used this access, and we have now revoked any technical capability they may have had to access any friends' data.

New apps that launched after April 30, 2014 were required to use our more restrictive platform APIs, which incorporated several key new elements, including:

- Institution of a review and approval process, called App Review (also called Login Review), for any app seeking to operate on the new platform that would request access to data beyond the user's own public profile, email address, and a list of friends of the user who had installed and authorized the same app;

- Generally preventing new apps on the new platform from accessing friends data without review; and

- Providing users with even more granular controls over their permissions as to what categories of their data an app operating on the new platform could access.

Our investigation is ongoing and as part of it we are taking a close look at applications that had access to friends data under Graph API V1 before we made technical changes to our platform to change this access.

The App Review process introduced in 2014 required developers who create an app that asks for more than certain basic user information to justify the data they are looking to collect and how they are going to use it. Facebook then reviewed whether the developer has a legitimate need for the data in light of how the app functions. Only if approved following such review can the app ask for a user's permission to get their data. Facebook has rejected more than half of the apps submitted for App Review between April 2014 and April 2018, including Kogan's second app. We are changing Login so that the only data that an app can request without app review will include name, profile photo, and email address.

We review apps to ensure that the requested permissions clearly improve the user experience and that the data obtained is tied to an experience within the app. We conduct a variety of manual and automated checks of applications on the platform for Policy compliance, as well as random sampling. When we find evidence of or receive allegations of violations, we investigate and, where appropriate, employ a number of measures, including restricting applications from our platform, preventing developers from building on our platform in the future, and taking legal action where appropriate.

Separately, in April, we found out that a feature that lets users look someone up by their phone number and email may have been misused by browsers looking up people's profiles in large volumes with phone numbers they already had. When we found out about the abuse, we shut this feature down. In the past, we have been aware of scraping as an industry issue, and have dealt with specific bad actors previously.

b. While the company represents that users could choose what information—if any—to share with Facebook, what steps could Facebook have taken, between 2007–2014, to better inform its users that their privacy settings could result in their Facebook content being scraped by third-parties when their friends used an app?

We believe that it's important to communicate with people about the information that we collect and how people can control it. That is why we work hard to provide this information to people in a variety of ways: in our Data Policy, and in Privacy Basics, which provides walkthroughs of the most common privacy questions we receive. Beyond simply disclosing our practices, we also think it's important to give people access to their own information, which we do through our Download Your Information and Access Your Information tools, Activity Log, and Ad Preferences, all of which are accessible through our Privacy Shortcuts tool. We also provide information about these topics as people are using the Facebook service itself.

We've heard loud and clear that privacy settings and other important tools are too hard to find and that we must do more to keep people informed. So, we're taking additional steps to put people more in control of their privacy. For instance, we redesigned our entire settings menu on mobile devices from top to bottom to make things easier to find. We also created a new Privacy Shortcuts in a menu where users can control their data in just a few taps, with clearer explanations of how our controls work. The experience is now clearer, more visual, and easy-to-find. Furthermore, we also updated our terms of service that include our commitments to everyone using Facebook. We explain the services we offer in language that's easier to read. We also updated our Data Policy to better spell out what data we collect and how we use it in Facebook, Instagram, Messenger, and other products.

People own what they share on Facebook, and they can manage things like who sees their posts and the information they choose to include on their profile.

Any person can see each of the specific interests we maintain about them for advertising by visiting Ads Preferences, which lets people see what interests we use to choose ads for them—and to edit or delete these interests. They can choose not to see ads from a particular advertiser or not to see ads based on their use of third-party websites and apps. They also can

choose not to see ads off Facebook that are based on the interests we derive from their activities on Facebook.

Our Download Your Information or "DYI" tool is Facebook's data portability tool and was launched many years ago to let people access and download many types of information that we maintain about them. The data in DYI and in our Ad Preferences tool contain each of the interest categories that are used to show people ads, along with information about the advertisers that are running ads based on their use of an advertiser's website or app. People also can choose not to see ads from those advertisers. We recently announced expansions to Download Your Information, which, among other things, will make it easier for people to see their data, delete it, and easily download and export it. More information is available at https://newsroom.fb.com/news/2018/04/new-privacy-protections/.

We have also introduced Access Your Information, a new tool that builds on the functionality we provide in Download Your Information. This feature provides a new way for people to access and manage their information. Users can go here to delete anything from their timeline or profile that they no longer want on Facebook. They can also see their ad interests, as well as information about ads they've clicked on and advertisers who have provided us with information about them that influence the ads they see. From here, they can go to their ad settings to manage how this data is used to show them ads.

And we recently announced plans to build Clear History. This feature will enable users to see the websites and apps that send us information when they use them, clear this information from their accounts, and turn off our ability to store it associated with their accounts going forward. Apps and websites that use features such as the Like button or Facebook Analytics send us information to make their content and ads better. We also use this information to make users' experiences on Facebook better. If a user clears their history or uses the new setting, we'll remove identifying information so a history of the websites and apps they've used won't be associated with their account. We'll still provide apps and websites with aggregated analytics—for example, we can build reports when we're sent this information so we can tell developers if their apps are more popular with men or women in a certain age group. We can do this without storing the information in a way that's associated with a user's account, and as always, we don't tell advertisers who a user is.

c. Did Facebook have a duty to inform users about scraping by third-parties?

Facebook allows people to view, manage, and remove the apps that they have logged into with Facebook through the App Dashboard. We recently prompted everyone to review their App Dashboard as a part of a Privacy Checkup, and we also provided an educational notice on Facebook to encourage people to review their settings. More information about how users can manage their app settings is available at https://www.facebook.com/help/218345114850283?helpref=about_content.

The categories of information that an app can access is clearly disclosed before the user consents to use an app on the Facebook platform. Users can view and edit the categories of information that apps they have used have access to through the App Dashboard.

In addition, Facebook notifies users in accordance with its obligations under applicable law and has also notified people in cases where there was no legal obligation to do so but we nevertheless determined it was the right thing to do under the circumstances.

d. What was the notification process if user data was scraped by a third-party in violation of the Terms of Service, under Facebook's policies, between 2014 and 2016? Under the company's new policy and terms of service, when does user notification come into play?

See Response to Question 2(c).

e. In the case of such scraping in violation of Facebook's Terms of Service, why would a user not be notified? Was any entity or person outside of Facebook ever notified about a breach of the Terms of Service? If yes, please identify the party, the timing, and the method of notification.

See Response to Question 2(c).

f. Which company executive(s) at Facebook were responsible for the decision not to notify users affected in 2015?

When Facebook learned about Kogan's breach of Facebook's data use policies in December 2015, we took immediate action. The company retained an outside firm to assist in investigating Kogan's actions, to demand that Kogan and each party he had shared data with delete the data and any derivatives of the data, and to obtain certifications that they had done so. Because Kogan's app could no longer collect most categories of data due to changes in Facebook's platform, our highest priority at that time was ensuring deletion of the data that Kogan may have accessed before these changes took place. With the benefit of hindsight, we wish we had notified people whose information may have been impacted. Facebook has since notified all people potentially impacted with a detailed notice at the top of their News Feed.

g. Is data scraping ever consistent with Facebook's own policies and, if so, please identify the specific policies?

Facebook's policies regarding third-party usage of its platform technologies have prohibited—and continue to prohibit—third-party app developers from selling or licensing user data accessed from Facebook and from sharing any user data accessed from Facebook with any ad network, data broker or other advertising or monetization-related service.

h. Facebook has opened an investigation into whether Cambridge Analytica still holds Facebook data after having promised they deleted it years ago. Will this investigation continue now that the company has announced it will shut down? If yes, how will the company inform the public about the results of the investigation?

Based on recent allegations, we have reopened our investigation into the veracity of these certifications and have hired a forensic auditor to conduct a forensic audit of Cambridge Analytica's systems. We are currently paused on the audit at the request of the UK Information

Commissioner's Office request, which is conducting a regulatory investigation into Cambridge Analytica (based in the UK), and we hope to move forward with that audit soon. Where we find evidence that these or other apps did misuse data, we will ban them from the platform and tell people who used or may have had data shared with the app.

i. Can Facebook enforce its own Terms of Service? Please enumerate the specific ways in which the company can enforce its terms and corporate policies, including any examples of successful or failed enforcement.

We use a variety of tools to enforce Facebook policies against violating parties, including developers. We review tens of thousands of apps per year and regularly disapprove noncompliant apps as part of our proactive review process. We also use tools like cease-and-desist letters, account suspensions, letter agreements, and civil litigation. For example, since 2006, Facebook has sent over 1,150 cease-and-desist letters to over 1,600 targets. In 2017, we took action against about 370,000 apps, ranging from imposing certain restrictions to removal of the app from the platform. Moreover, we have required parties who have procured our data without authorization to delete that data. We have invested significant resources in these efforts. Facebook is presently investigating apps that had access to large amounts of information before we changed our platform policies in 2014 to significantly reduce the data apps could access. As of June 2018, around 200 apps (from a handful of developers: Kogan, AIQ, Cube You, the Cambridge Psychometrics Center, myPersonality, and AIQ) have been suspended—pending a thorough investigation into whether they did in fact misuse any data.

Additionally, we have suspended an additional 14 apps, which were installed by around one thousand people. They were all created after 2014, after we made changes to more tightly restrict our platform APIs to prevent abuse. However, these apps appear to be linked to AIQ, which was affiliated with Cambridge Analytica. So, we have suspended them while we investigate further. Any app that refuses to take part in or fails our audit will be banned.

j. What are the technical limitations on limiting how third-party app developers use Facebook data? For instance, would it be possible to track the metadata associated with Facebook information to determine if it had been shared inappropriately?

Recently, we announced a number of additional steps we're taking to address concerns raised by Kogan's app.

- **Review our platform.** We will investigate all apps that had access to large amounts of data before the platform changes we announced in 2014, and we will audit any app where we identify suspicious activity. If we identify misuses of data, we'll take immediate action, including banning the app from our platform and pursuing legal action if appropriate.

- **Tell people about data misuse.** We will tell people about apps that have misused their data.

- **Turn off access for unused apps.** If someone has not used an app within the last three months, we will turn off the app's access to their data.

- **Restrict Facebook Login data.** We are changing Login, so that the only data that an app can request without app review will include name, profile photo, and email address. Requesting any other data will require approval from Facebook. We will also no longer allow apps to ask for access to information like religious or political views, relationship status and details, custom friends lists, education and work history, fitness activity, book reading and music listening activity, news reading, video watch activity, and games activity. We will encourage people to manage the apps they use. We already show people what apps their accounts are connected to and allow them to control what data they've permitted those apps to use. But we're making it easier for people to see what apps they use and the information they have shared with those apps.

- **Reward people who find vulnerabilities.** We launched the Data Abuse Bounty program so that people can report to us any misuses of data by app developers.

- **Update our policies.** We have updated our terms and Data Policy to explain how we use data and how data is shared with app developers.

See Response to Question 2(a) for more detail.

k. Do you think Facebook made its practice of allowing third-party access to Facebook user data sufficiently clear to its users?

See Response to Question 2(b).

3. Please indicate the specific ways a Facebook user could find the list of third-party app developers who have access to their data in January 2018 and, separately, today? Does this list include, or did it ever include, a list of third-party apps friends of a Facebook user allowed to access that Facebook users' data?

a. Where can a user find information about how their data might be used by a third-party developer? Does Facebook inform its users – or must a user obtain that information directly from the developer?

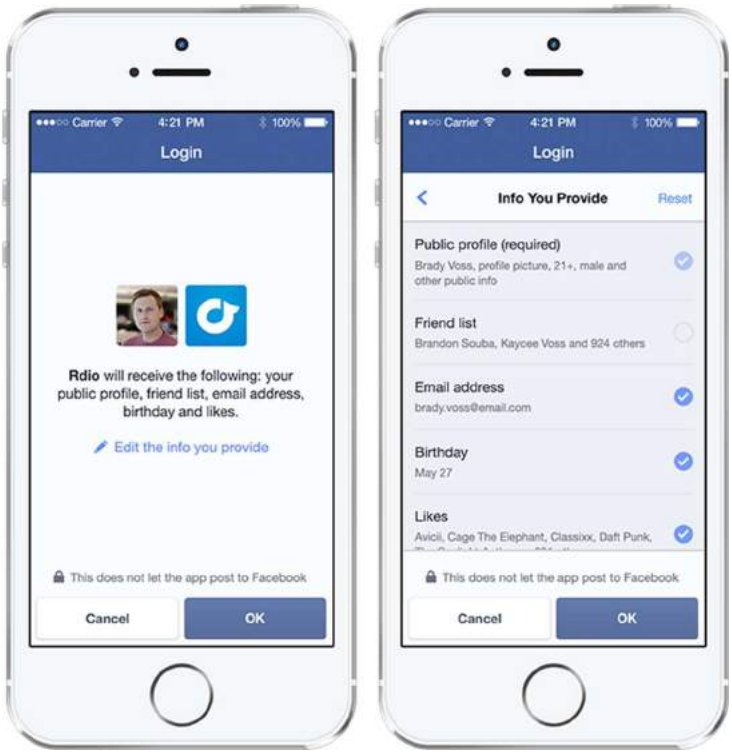
We encourage people to manage the apps they use. We already show people what apps their accounts are connected to and allow them to control what data they've permitted those apps to use. But we're making it easier for people to see what apps they use and the information they have shared with those apps.

4. Following the streamlining and simplification of the company's privacy policy and settings in April 2018, how many different pages or steps does a user have to visit to make decisions about the privacy controls for their data and whether apps have access to it?

a. Prior to the April 2018 changes, how many different pages or steps did a user have to visit or take?

b. How many times were the settings and locations changed for users between the launch of Facebook Platform and today?

Since the changes we introduced to platform in 2014, whenever a person first logs into a third-party app using Facebook Login, they are shown the data that the app is requesting access to and are asked to agree to or edit the information the app can access. Everyone has to go through this experience before using a third-party app that integrates Facebook Login. Prior to 2014, people were similarly prompted to agree to the data sharing when they first logged into the app, but we did not offer granular permissions to access specific data types. Here is an example of what the 2014 experience looked like:



If someone wants to later change the data an app has access to, remove the app, or opt out of the platform altogether those controls are available in Settings. It takes about 3-4 clicks to get to the controls depending upon the platform as described here: https://www.facebook.com/help/218345114850283. On April 9, 2018, we started showing people a link at the top of their News Feed so they can see what apps they use—and the information they have shared with those apps.

5. In the initial development the Facebook Platform, did you or anyone in senior management consider or review a plan to address potential misuse by app developers? If no, why not? If yes, what was the result of that consideration or

review? Did that plan consider the type of misuse perpetrated by Dr. Aleksandr Kogan?

As our founder and CEO described in his written testimony, Facebook is an idealistic and optimistic company. For most of our existence, we focused on all the good that connecting people can bring. As Facebook has grown, people everywhere have gotten a powerful new tool to stay connected to the people they love, make their voices heard, and build communities and businesses. But it's clear now that we didn't do enough to prevent these tools from being used for harm as well. That goes for fake news, foreign interference in elections, and hate speech, as well as developers and data privacy. We didn't take a broad enough view of our responsibility, and that was a big mistake.

In early 2014, Facebook introduced changes to provide users more choice and control over what information apps received, to reduce the amount of data that could be shared with third-party apps, and to establish a new review and approval process for any new apps that sought to request anything more than basic information about the installing user. These changes accompanied a new version of the platform API, called Graph API V2, which incorporated several key new elements. For more detail on the App Review process introduced in 2014, see Response to Question 2(a).

6. At launch of the Facebook Platform, did the company place any restrictions on what developers could do with Facebook user data?

a. If yes, what were those restrictions, and how did Facebook verify compliance? Who vetted this decision, including specific executive officers at the company? Who is responsible for enforcing compliance at Facebook? Has that role changed since 2007, and if so, how? Please describe.

b. If no, which specific executive officers were a part of the decision not to put limitations on developers use of Facebook data? Did Facebook anticipate potential, and reasonably foreseeable, misuse and what to do about it? Who vetted this decision – which specific executive officers at the company? Please describe.

c. How many third-party developers did Facebook take actions against until 2014 for violations of these restrictions?

See Response to Question 2(a).

7. At the April 11 hearing, Facebook announced audits of all developer apps to find out how many other incidents, similar to the Cambridge Analytica incident, may have happened on the platform. Will the company be transparent about the results of the audits? Will Facebook commit to provide this Committee with the results of the audit? Is Facebook conducting the audit itself or will you have an independent auditor involved? If Facebook intends to use an independent auditor, please identify the auditor.

We are in the process of investigating every app that had access to a large amount of information before we changed our Platform in 2014. The investigation process is in full swing, and it has two phases. First, a comprehensive review to identify every app that had access to this amount of Facebook data and to focus on apps that present reason for deeper investigation. And second, where we have concerns, we will conduct interviews, make requests for information (RFI)—which ask a series of detailed questions about the app and the data it has access to—and perform audits using expert firms that may include on-site inspections. We have large teams of internal and external experts working hard to investigate these apps as quickly as possible. As of early June 2018, thousands of apps have been investigated and around 200 apps have been suspended—pending a thorough investigation into whether they did in fact misuse any data. Where we find evidence that these or other apps did misuse data, we will ban them and let people know.

These apps relate to a handful of developers: Kogan, AIQ, Cube You, the Cambridge Psychometrics Center, and myPersonality, with many of the suspended apps being affiliated with the same entity. Many of these suspensions include apps that appear to be "test" apps that were never released to the public, and therefore would not have acquired significant user data, although our investigation into these apps is ongoing.

Additionally, we have suspended an additional 14 apps, which were installed by around one thousand people. They were all created after 2014, after we made changes to more tightly restrict our platform APIs to prevent abuse. However, these apps appear to be linked to AIQ, which was affiliated with Cambridge Analytica. So, we have suspended them while we investigate further. Any app that refuses to take part in or fails our audit will be banned.

We will commit to briefing your staff on future developments.

8. On the issue of audits, in 2011, Facebook signed a consent order with the FTC for privacy violations. Part of that consent order requires Facebook to submit third-party privacy audits to the FTC every two years.

a. Please provide a summary of all audits conducted in connection with the FTC consent decree.

To date, three independent privacy assessments prepared by PwC have been completed and submitted to the FTC: a 180-Day assessment report (dated April 16, 2013), a biennial report covering the period between February 12, 2013 and February 11, 2015 (dated April 13, 2015), and a biennial report covering the period between February 12, 2015 and February 11, 2017 (dated April 12, 2017). In each of these assessments, PwC determined that Facebook's privacy controls were operating with sufficient effectiveness to provide reasonable assurance to protect the privacy information covered under the FTC Consent Order, in all material respects.

b. Please provide this Committee with copies of all audits conducted.

The privacy assessments conducted by PwC contain both Facebook's and PwC's sensitive business information that are confidential in order to prevent competitive harm and to ensure the integrity of Facebook's privacy program, including the steps that we take to protect people's information. We have furnished these reports to the FTC and are prepared to review the

reports with regulators and lawmakers with appropriate assurances that confidential information or information that could be exploited to cause competitive harm or to circumvent Facebook's privacy protections will not be disclosed publicly.

9. How can companies that rely on user-generated data, like Facebook, make terms and conditions more accessible and understandable for individual users? Has Facebook conducted any research on the effectiveness of notice mechanisms for privacy settings and other terms and conditions? If yes, what were the results of that research?

We believe that it's important to communicate with people about the information that we collect and how people can control it. This is why we work hard to provide this information to people in a variety of ways: in our Data Policy, and in Privacy Basics, which provides walkthroughs of the most common privacy questions we receive. Beyond simply disclosing our practices, we also think it's important to give people access to their own information, which we do through our Download Your Information and Access Your Information tools, Activity Log, and Ad Preferences, all of which are accessible through our Privacy Shortcuts tool. We also provide information about these topics as people are using the Facebook service itself.

There is no single number that measures how much time people spend understanding how Facebook services work, in large part because Facebook seeks, as much as possible, to put controls and information in context within its service. While "up front" information like that contained in the terms of service are useful, research overwhelmingly demonstrates that in-product controls and education are the most meaningful to people and the most likely to be read and understood. On-demand controls are also important, and we recently redesigned our entire settings menu on mobile devices from top to bottom to make things easier to find. We also created a new Privacy Shortcuts, a menu where people can control their data in just a few taps, with clearer explanations of how our controls work. The experience is now clearer, more visual, and easy-to-find.

Improving people's understanding of how digital services work is an industry-wide challenge that we are highly committed to addressing. That's why, over the last 18 months, we've run a global series of design workshops called "Design Jams", bringing together experts in design, privacy, law, and computer science to work collaboratively on new and innovative approaches. These workshops have run in Paris, London, Dublin, Berlin, Sao Paolo, Hong Kong, and other cities, and included global regulators and policymakers. At these workshops, expert teams use "people centric design" methods to create innovative new design prototypes and experiences to improve transparency and education in digital services. These workshops inform Facebook's constantly-improving approach.

In recognition of the need for improved approaches to data transparency across all digital services, working with partners from academia, design, and industry we recently launched TTC Labs, a design innovation lab that seeks to improve user experiences around personal data. TTC Labs is an open platform for sharing and innovation and contains insights from leading experts in academia, design, and law, in addition to prototype designs from the Design Jams, template services and open-source toolkits for people-centric design for transparency, trust and control of data. Working collaboratively, and based on open-source approaches, TTC Labs seeks to pioneer

new and more people-centric best practices for people to understand how their data is used by digital services, in ways that they find easy to understand and control.

Facebook is highly committed to improving people's experience of its own services as well as investing in new innovations and approaches to support improvements across the industry.

10. In 2013, did Facebook have an approval process for third-party app developers seeking to use, or already operating on, the Facebook Platform? If so, what was that approval process? Please describe the process in detail.

a. Was it Facebook's practice in 2013 to allow app developers to collect data on "friends" even if those users ("friends") did not download or use the app?

See Response to Question 2(a).

11. Prior to the April 11 hearing, there were several news reports about CubeYou and its violation of Facebook's policies. While Aleksandr Kogan's app "thisisyourdigitallife" was active on your platform, did the company ever audit apps to determine if any were in violation of Facebook's policies? If so, how many audits were conducted? Did Facebook ever audit "thisisyourdigitallife"? If yes, what were the results of that audit? If not, why not?

On December 11, 2015, *The Guardian* published an article reporting that Kogan and his company, GSR, may have passed information the app had obtained from Facebook users to SCL Elections Ltd. (SCL)/Cambridge Analytica. Kogan and his company violated Facebook's Platform Policies, which explicitly prohibited selling user data accessed from Facebook and from sharing any user data accessed from Facebook with any ad network, data broker or other advertising or monetization related service.

For this reason, Facebook immediately banned the app from our platform and investigated what happened and what further action we should take to enforce our Platform Policies. Facebook also contacted Kogan/GSR and demanded that they explain what data they collected, how they used it, and to whom they disclosed it. Facebook further insisted that Kogan and GSR, as well as other persons or entities to whom they had disclosed any such data, account for and irretrievably delete all such data and information.

Facebook also contacted Cambridge Analytica to investigate the allegations reflected in the reporting. On January 18, 2016, Cambridge Analytica provided written confirmation to Facebook that it had deleted the data received from Kogan and that its server did not have any backups of that data. On June 11, 2016, Kogan executed certifications of deletion on behalf of himself and GSR. The certifications also purported to identify all of the individuals and entities that had received data from GSR (in addition to Kogan and his lab), listing the following: SCL, Eunoia Technologies (a company founded by Christopher Wylie), and a researcher at the Toronto Laboratory for Social Neuroscience at the University of Toronto. On July 7, 2016, a representative of the University of Toronto certified that it deleted any user data or user-derived data. On August 16, 2016, Eunoia (executed by Eunoia Founder Christopher Wylie) certified that it deleted any user and user-derived data. On September 6, 2016, counsel for SCL informed

counsel for Facebook that SCL had permanently deleted all Facebook data and derivative data received from GSR and that this data had not been transferred or sold to any other entity. On April 3, 2017, Alexander Nix, on behalf of SCL, certified to Facebook, that it deleted the information that it received from GSR or Kogan.

Because all of these concerns relate to activity that took place off of Facebook and its systems, we have no way to confirm whether Cambridge Analytica may have Facebook data without conducting a forensic audit of its systems. Cambridge Analytica has agreed to submit to a forensic audit, but we have not commenced that yet due to a request from the UK Information Commissioner's Office, which is simultaneously investigating Cambridge Analytica (which is based in the UK). And even with an audit, it may not be possible to determine conclusively what data was shared with Cambridge Analytica or whether it retained data after the date it certified that data had been deleted.

The existing evidence that we are able to access supports the conclusion that Kogan only provided SCL with data on Facebook users from the United States. While the accounts of Kogan and SCL conflict in some minor respects not relevant to this question, both have consistently maintained that Kogan never provided SCL with any data for Facebook users outside the United States. These consistent statements are supported by a publicly released contract between Kogan's company and SCL.

12. The European Union has new privacy rules going into place next month - does the company believe that if those rules would have been in place in 2013 here in the U.S. that they would have prevented the situation with Aleksandr Kogan and the "thisisyourdigitallift" app scraping user data and sharing it in violation of Facebook's terms and conditions?

The new European privacy rules (GDPR) and indeed the privacy rules that preceded the GDPR, oblige data controllers to have a valid legal basis to share personal data. When our users choose to share their Facebook data with app developers, those app developers receive that data as independent third-party data controllers and bear legal responsibility for lawful processing of that data and keeping that data secure, including under GDPR. In addition, to the extent third parties obtain data from those app developers in circumstances constituting a notifiable data breach, the notification obligation falls on the developer.

In this way any obligations under the GDPR (e.g., the unauthorized sharing of European user's data collected by Kogan's app with third parties and/or the obligation to notify regulators and people of a data breach) would have fallen on Kogan as data controller. However, it is not clear that these legal obligations would have prevented Kogan's actions, since he faced similar legal obligations under the UK Data Protection Act at the time.

However, with the benefit of hindsight, we nonetheless wish we had notified people whose information may have been impacted, even though there was no legal obligation to do so. Facebook has since notified all people potentially impacted with a detailed notice at the top of News Feed.

13. Many people get their news and information on current events on the Facebook Platform. How does Facebook decide what information to allow on its platform and what information violates its terms and conditions?

a. Does Facebook make judgement calls as to what information it should allow on its platform? Please describe in detail the criteria for those decisions.

b. Are these decisions made by humans or by algorithms? Please describe,

c. Have you, Mr. Zuckerberg, directed or approved any of these policies? Please describe.

Facebook is a distribution platform that reflects the conversations already taking place in society. We want Facebook to be a place where people can discover more news, information, and perspectives, and we are working to build products that help.

To fight the spread of false news, Facebook uses a mix of technological solutions, human reviewers, and educational programs that promote news literacy. The Facebook community plays an important role, too: people can give feedback that a post on Facebook contains false news by clicking the three dots at the top of the post.

A user's News Feed is made up of stories from their friends, Pages they've chosen to follow and groups they've joined. News Feed considers thousands of signals to surface the content that's most relevant to each person who uses Facebook. Our employees don't determine the ranking of any specific piece of content. Ranking is the process we use to organize all of those stories so that users can see the most relevant content at the top, every time they open Facebook. Ranking has four elements: the available inventory of stories; the signals, or data points that can inform ranking decisions; the predictions we make, including how likely we think a user is to comment on a story, share with a friend, etc.; and a relevancy score for each story. Signals include a wide range of things, from how old a given post is and who posted it to little things, like how fast a user's internet connection is right now or what kind of phone the user is using. To help the community understand how News Feed works and how changes to News Feed affect their experience on Facebook, we publish a regularly-updated News Feed FYI blog (https://newsroom.fb.com/news/category/inside-feed/) where our team shares details of significant changes.

One application of these signals is to help determine whether a post might be clickbait, false news, or other types of inauthentic content. Today, in the US, the signals for false news include things like whether the post is being shared by a Page that's spread a lot of false news before, whether the comments on the post include phrases that indicate readers don't believe the content is true, or whether someone in the community has marked the post as false news.

Facebook uses a machine learning classifier to compile all of those misinformation signals and—by comparing a given post to past examples of false news—make a prediction: "How likely is it that a third-party fact-checker would say this post is false?" (Facebook uses classifiers for a lot of different things, like predicting whether a post is clickbait or contains nudity; you can read more in this roundtable interview from *Wired* (https://www.wired.com/story/how-facebook-wants-to-improve-the-quality-of-your-news-

feed/)). The classifier's predictions are then used to determine whether a given piece of content should be sent to third-party fact-checkers. If a fact-checker rates the content as false, it will get shown lower in people's News Feeds and additional reporting from fact-checkers will be provided.

More feedback from more people helps make the classifier more accurate, but feedback in and of itself doesn't trigger the fact-checking process. That's because people may mean different things when they mark a post—they might disagree with the content, or dislike the Page or person posting it. That's why the misinformation classifier takes a range of things into account—though user feedback is one of the most important.

Facebook is continually working to improve its classifiers. Classifiers learn to make their predictions by looking at a variety of examples of the thing they're trying to identify—so the more data collected, the better the classifier gets and the more precisely it can sift through signals to find meaningful patterns. Facebook also has to make sure that it's serving people in different cultural and linguistic contexts, so classifiers also have to be trained to be sensitive to regional and linguistic differences, as well as to cultural norms. This means that the variety of misinformation signals Facebook relies upon in any given country, and the weight that is assigned to each, is not static.

14. There have been recent reports that indicate Facebook was planning to obtain patient data from hospitals and other healthcare organizations. Did Facebook or any other healthcare organization analyze how this data sharing would comply with federal privacy laws such as the Health Insurance Portability and Accountability Act (HIPPA)?

a. What plans, if any, did Facebook have to notify users that their data would be matched with their health information?

b. Press reports also indicated the plan was for health organizations to share patient information with certain details, such as the patient's name, obscured, and that Facebook planned to use a technique called "hashing" to match the patient's medical records with the patient's Facebook records to generate recommendations for customized care for the patient. Given that computers would use an algorithm to match the patient information with the Facebook user data for that patient, is it possible that patient data could have been re-identified by others as well? If not, why not? Please describe in detail.

c. Given how Facebook has improperly shared user data and failed to ensure that personal data is adequately protected, how did Facebook plan to prevent a patient's health data from ending up with a firm like Cambridge Analytica?

d. How did Facebook plan on using the information it generated from this process?

e. One press article indicated that patients' names and other identifiable information would be withheld from both parties. Wouldn't the patient have to be re-identified by either the health care organization or Facebook to use the results from this matching process to customize the care for that patient?

f. Was Facebook going to share its user data with health care organizations after it had matched the patient's medical record to the patient's user data on Facebook?

g. How was this information going to be shared with patients?

Facebook was exploring this type of data sharing because of the general health benefits to having a close-knit circle of family and friends and the need for more research on the impact of social connection on health. Deeper research into this link is needed to help medical professionals develop specific treatment and intervention plans that take social connection into account. With this in mind, last year Facebook began discussions with leading medical institutions, including the American College of Cardiology and the Stanford University School of Medicine, to explore whether scientific research using fully-anonymized Facebook data could help the medical community advance our understanding in this area. This work did not progress past the planning phase, and we have not received, shared, or analyzed anyone's data.

In March we decided that we should pause these discussions so we can focus on other important work, including doing a better job of protecting people's data and being clearer with them about how that data is used in our products and services.

Our Data Policy has explained that we have engaged in research collaborations for several years. As part of a general effort to be more transparent, we updated our Data Policy recently to provide additional detail on a range of practices, including academic research. We also explain this in other ways, including announcements in our Newsroom and in a dedicated website providing more information about research at Facebook.

15. In Facebook's previous data policy, last updated in 2016, it is noted: "When you use third-party apps, websites or other services that use, or are integrated with, our Services, they may receive information about what you post or share." Please explain what you mean by "integrated with."

We impose strict restrictions on how our partners can use and disclose the data we provide. Our Data Policy makes clear the circumstances in which we work with third parties who help us provide and improve our Products or who use Facebook Business Tools to grow their businesses, which makes it possible to operate our companies and provide free services to people around the world.

When people choose to use third-party apps, websites, or other services that use, or are integrated with, our Products, they can receive information about what users post or share. For example, when users play a game with their Facebook friends or use a Facebook Comment or Share button on a website, the game developer or website can receive information about the users' activities in the game or receive a comment or link that users share from the website on Facebook. Also, when users download or use such third-party services, they can access users'

public profile on Facebook, and any information that users share with them. Apps and websites that people use may receive their list of Facebook friends if they choose to share it with them. But apps and websites that people use will not be able to receive any other information about their Facebook friends from users, or information about any of the users' Instagram followers (although friends and followers may, of course, choose to share this information themselves). Information collected by these third-party services is subject to their own terms and policies.

Separately, Facebook entered into partnerships with businesses, primarily devices and operating systems, to integrate Facebook and Facebook features on to those companies' devices and other products.

Today, most people access Facebook through mobile applications we have developed for the world's leading smartphone operating systems, Apple's iOS and Google's Android, or our website (www.facebook.com). Apple and Google provide online stores that enable users of their operating systems to easily download third-party software applications—or apps—onto their devices, including versions of Facebook that we build for those devices.

The partnerships—which we call "integration partnerships"—began before iOS and Android had become the predominant ways people around the world accessed the internet on their mobile phones. People went online using a wide variety of text-only phones, feature phones, and early smartphones with varying capabilities. In that environment, the demand for internet services like Facebook, Twitter, and YouTube outpaced our industry's ability to build versions of our services that worked on every phone and operating system. As a solution, internet companies often engaged device manufacturers and other partners to build ways for people to access their experiences on a range of devices and products.

We engaged companies to build integrations for a variety of devices, operating systems and other products where we and our partners wanted to offer people a way to receive Facebook or Facebook experiences. These integrations were built by our partners, for our users, but approved by Facebook. They included:

- *Facebook-branded apps*: Some partners built versions of Facebook for their device, operating system, or product that replicated essential Facebook features that we built directly on the Facebook website and in our mobile apps.

- *Social Networking Service Hubs*: Some partners built "hubs" into their products, where people could see notifications from their friends or the people they followed on Facebook, MySpace, Twitter, Google, and other services. People often could also use these integrations to post on these social networking services.

- *Syncing Integrations*: Some partners enabled people to sync their Facebook data (e.g., photos, contacts, events, and videos) with their device in order to integrate Facebook features on their device. This allowed people to, for example, easily upload pictures to Facebook and to download their Facebook pictures to their phones, or to integrate their Facebook contacts into their address book.

- *USSD Services*: Some partners developed USSD services, which are services that provided Facebook notifications and content via text message. This was useful for feature phones that did not have the ability to connect to the internet; it particularly helped us bring Facebook to people in the developing world.

To provide these experiences, we permitted partners to use certain Facebook application programming interfaces (or "APIs"), which are basic technologies that enable two computing systems to "talk" to one another. In general, partners were licensed to use these APIs solely for providing specific integrations, approved by Facebook, to Facebook users who requested these services on the partners' products. These integrations were reviewed by Facebook, which had to approve implementations of the APIs. Typically, these apps were reviewed and approved by members of our partnerships and engineering teams.

In these and other ways, these partnerships differed significantly from third-party app developers' use of published APIs to build apps for consumers on Facebook's developer platform. As we explain below, third-party app developers use the information they receive in order to build their own experiences, not to build Facebook-approved applications for purposes designated by Facebook. Integration partners were not permitted to use data received through Facebook APIs for independent purposes unrelated to the approved integration without user consent.

Our integration partnerships are fundamentally different from the relationships Facebook has with other developers that use our developer platform:

First, our integration partnerships involved engaging select partners to build ways for Facebook users to receive Facebook or Facebook features. As the New York Times notes, we partnered with the maker of Blackberry to provide Facebook services on that device. We also partnered with companies such as Apple, Microsoft and Samsung to help us provide Facebook features and functionality on their devices and in their software. Our developer platform, on the other hand, is designed to enable developers to use information provided by Facebook users to build their own unique experiences under the terms and policies they provide to their users, rather than to mimic core Facebook experiences—something that Facebook's developer terms (the "Platform Policy") make clear.

Second, our integration partnerships were managed by our partnerships and engineering teams, which reviewed and approved how licensed APIs were integrated into the partner's products. By contrast, our Developer Operations ("Dev Ops") team oversees third-party developers, which determine for themselves how they will build their apps - subject to Facebook's general Platform Policies and Dev Ops approval for apps seeking permission to use most published APIs.

Third, these partnerships typically were defined by specially-negotiated agreements that provided limited rights to use APIs to create specific integrations approved by Facebook, not independent purposes determined by the partner.

The list below shows the 52 companies that Facebook authorized to build versions of Facebook or Facebook features for their devices and products.

Facebook already has discontinued 38 of these 52 partnerships, and will shut down an additional seven by the end of July 2018 and another one by the end of October 2018. Three partnerships will continue: (1) Tobii, an accessibility app that enables people with ALS to access Facebook; (2) Amazon; and (3) Apple, with whom we have agreements that extend beyond October 2018. We also will continue partnerships with Mozilla, Alibaba and Opera— which enable people to receive notifications about Facebook in their web browsers—but their integrations will not have access to friends' data.

1. Accedo
2. Acer
3. Airtel
4. Alcatel/TCL
5. Alibaba**
6. Amazon*
7. Apple*
8. AT&T
9. Blackberry
10. Dell
11. DNP
12. Docomo
13. Garmin
14. Gemalto*
15. HP/Palm
16. HTC
17. Huawei
18. INQ
19. Kodak
20. LG
21. MediaTek/ Mstar
22. Microsoft
23. Miyowa /Hape Esia
24. Motorola/Lenovo
25. Mozilla**
26. Myriad*
27. Nexian
28. Nokia*
29. Nuance
30. O2
31. Opentech ENG
32. Opera Software**
33. OPPO
34. Orange
35. Pantech
36. PocketNet
37. Qualcomm
38. Samsung*
39. Sony

40. Sprint
41. T-Mobile
42. TIM
43. Tobii*
44. U2topia*
45. Verisign
46. Verizon
47. Virgin Mobile
48. Vodafone*
49. Warner Bros
50. Western Digital
51. Yahoo*
52. Zing Mobile*

*Note: * denotes partnerships that we are still in the process of ending (with the exception of Tobii, Apple and Amazon, which will continue beyond October 2018). **denotes partnerships that will continue but integrations will not have access to friends' data. All other partnerships on the list have already been discontinued. It is important to note that the list above is comprehensive to the best of our ability. It is possible we have not been able to identify some integrations, particularly those made during the early days of our company when our records were not centralized. It is also possible that early records may have been deleted from our system.*

To date, our communications with the Committee—including Mark Zuckerberg's written testimony and his answers to questions in the hearing—have focused on apps offered to consumers on our developer platform because this was the product area implicated by the Cambridge Analytica matter. However, we wanted to address recent press reports regarding device integrations. We hope this additional detail is helpful to the Committee. We would, of course, welcome the opportunity to speak further about these matters.

a. Does this include just having the Facebook "Like" button on a webpage?

See Response to Question 15.

b. The Data Policy also said: "We collect information when you visit or use third- party websites and apps that use our Services (e.g. when they offer our Like button or Facebook Log In or use our measurement and advertising services)." Does this imply that Facebook has a nexus to collect information about its users from every single website that uses the Facebook Like button? Please explain.

See Response to Question 15.

c. What is the percentage of unaffiliated Internet websites on which Facebook tracks user activity or behavior?

Facebook does not publish tracking software. When people visit apps or websites that feature our technologies—like the Facebook Like or Comment button—our servers automatically log (i) standard browser or app records of the fact that a particular device or user visited the website or app (this connection to Facebook's servers occurs automatically when a person visits a website or app that contains our technologies, such as a Like button, and is an inherent function of internet design); and (ii) any additional information the publisher of the app or website chooses to share with Facebook about the person's activities on that site (such as the fact that a purchase was made on the site).

This is a standard feature of the internet, and most websites and apps share this same information with multiple different third-parties whenever people visit their website or app. For example, the House Energy and Commerce Committee's website shares information with Google Analytics to help improve the site. This means that, when a person visits the Committee's website, it sends browser information about their visit to that third party. More information about how this works is available at https://newsroom.fb.com/news/2018/04/data-off-facebook/.

During the week prior to April 16, 2018, on sites that use Facebook services: the Like button appeared on 8.4 million websites, the Share button on 931,000 websites covering 275 million webpages, and there were 2.2 million Facebook pixels installed on websites.

16. There have been numerous reports of fake Facebook accounts and, understanding that "views" is what is important in this space, are fake accounts being used to increase Facebook's advertising statistics? What verification methods exist for advertisers to confirm data provided by Facebook about the effectiveness of advertisements placed on Facebook? Please describe in detail.

We have a team dedicated to preventing and detecting fake traffic generating "views" for ads. We use multiple means including AI to detect invalid traffic generated by bots that may increase advertising statistics. We also block malicious sources that are generating invalid traffic.

We also have a process for advertisers to reach out to us and share their insights about the traffic they're seeing. We investigate such requests and get back to advertisers.

We comply with industry standards (Media Ratings Council) to detect and eliminate invalid traffic from our advertising platform. Advertisers are not billed for traffic identified as invalid.

17. We often hear that algorithms described as a black box – meaning, we know what information goes in the algorithm and what comes out, but we do not know how that information is processed by the algorithm. Is Facebook able to audit its algorithms to know how they operate? How can the public be certain the algorithms are not promoting certain content over others outside the terms and conditions publicized by Facebook?

We are focused on both the technical and the ethical aspects of artificial intelligence and algorithms. We believe these two should go hand-in-hand together in order to fulfill our

commitment to being fair, transparent and accountable in our development and use of AI. Facebook has AI teams working on developing the philosophical, as well as technical, foundations for this work. Facebook is also one of the co-founders and members of the Partnership on AI (PAI), a collaborative and multi-stakeholder organization established to study and formulate best practices on AI technologies, to advance the public's understanding of AI, and to serve as an open platform for discussion and engagement about AI and its influences on people and society. The thematic pillars that structure the work we're doing in the scope of the PAI—safety, fairness, transparency and accountability—are the principles that we believe industry should follow and promote when building and deploying AI systems. The PAI's Fair, Transparent and Accountable AI Working Group is also working alongside industry, academia, and civil society to develop best practices around the development and fielding of fair, explainable, and accountable AI systems.

We believe that over the long term, building AI tools is the scalable way to identify and root out most content that violates our policies. We are making substantial investments in building and improving these tools. We already use artificial intelligence to help us identify threats of real world harm from terrorists and others. For example, the use of AI and other automation to stop the spread of terrorist content is showing promise. Today, 99 percent of the ISIS and Al Qaeda related terror content we remove from Facebook is content we detect before anyone in our community has flagged it to us, and in some cases, before it goes live on the site. We do this primarily through the use of automated systems like photo and video matching and text-based machine learning. We also use AI to help find child exploitation images, hate speech, discriminatory ads, and other prohibited content.

18. Does Facebook have an inherent responsibility to protect people's personal information, and can you comment on whether or not Facebook has proprietary rights over some, if not all, of that information?

A user owns the information they share on Facebook. This means they decide what they share and who they share it with on Facebook, and they can change their mind. We believe that everyone has the right to expect strong protections for their information, and that we also need to do our part to help keep our community safe, in a way that's consistent with people's privacy expectations. We've recently announced several steps to give people more control over their privacy, including a new Privacy Shortcuts tool that we're rolling out now to give people information about how to control their information, including choosing who can see what they post and adding protections like two-factor authentication to their account. People can learn more about how to protect their privacy in our updated Data Policy and in our Privacy Basics feature (https://www.facebook.com/about/basics). Moreover, we require websites and apps who use our tools to tell users they're collecting and sharing their information with us, and to get users' permission to do so.

19. Flow does Facebook plan to reconcile its ability to operate at a quality level you deem efficient while allowing users to share information with their friends and family with peace of mind?

a. Must users sacrifice their data, or control of their data outside the service, in order to participate on your network?

Privacy is at the core of everything we do, and our approach to privacy starts with our commitment to transparency and control. Our threefold approach to transparency includes, first, whenever possible, providing information on the data we collect and use and how people can control it in context and in our products. Second, we provide information about how we collect and use data in our user agreements and related educational materials. And third, we enable people to learn more about the specific data we have about them through interactive tools such as Download Your Information, which lets people download a file containing data that they may want to take to another service, and Access Your Information, a tool we are launching that will let people more easily access and manage their data on Facebook.

Our approach to control is based on the belief that people should be able to choose who can see what they share and how their data shapes their experience on Facebook. People can control the audience for their posts and the apps that can receive their data. They can see and delete the history of their activities on Facebook, and, if they no longer want to use Facebook, they can delete their account and the data associated with it. Of course, we recognize that controls are only useful if people know how to find and use them. That is why we continuously deliver in-product educational videos in people's News Feeds on important privacy topics. We are also inviting people to take our Privacy Checkup—which prompts people to review key data controls—and we are sharing privacy tips in education campaigns off of Facebook, including through ads on other websites. To make our privacy controls easier to find, we are launching a new settings menu that features core privacy settings in a single place. We are always working to help people understand and control how their data shapes their experience on Facebook.

20. Does Facebook record and store any audio files from Facebook users? Does the company record and store any video files from Facebook users?

No, Facebook does not engage in these practices or capture data from a microphone or camera without consent. Of course, we do allow people to take videos on their devices and share those on our platform.

21. What level of control do Facebook users have over the information they provide to Facebook and how has that changed since the Cambridge Analytica incident?

See Response to Question 19.

Our policies limit our retention of the data that we receive in several ways. Specifically, we store data until it is no longer necessary to provide our services and Facebook products, or until a person's account is deleted—whichever comes first. This is a case-by-case determination that depends on things like the nature of the data, why it is collected and processed, and relevant legal or operational retention needs. For example, if a user posts something on their Facebook profile, then that information would be retained until they delete it or until they delete their account.

We also have other policies that are designed to limit our retention of other types of information about people. For example, if a user clicks a "Like" button that appears on a third-party site, we may use that information to show the person a more personalized experience on Facebook, to help maintain and improve our service, and to protect both the user and Facebook

from malicious activity. We delete or anonymize the URL where the Like occurred within 90 days.

In general, when a user deletes their account, we delete things they have posted, such as their photos and status updates, and they won't be able to recover that information later. (Information that others have shared about them isn't part of their account and won't be deleted.)

There are some limited exceptions to these policies: For instance, information can be accessed and preserved for an extended period when it is the subject of a legal request or obligation, governmental investigation, or investigations of possible violations of our terms or policies, or otherwise to prevent harm. We also retain information from accounts disabled for terms violations for at least a year to prevent repeat abuse or other term violations.

Particularly in the past few months, we've realized that we need to take a broader view of our responsibility to our community. Part of that effort is continuing our ongoing efforts to identify ways that we can improve our privacy practices. This includes restricting the way that developers can get information from Facebook and announcing plans to build Clear History, a new feature that will enable users to see the websites and apps that send us information when they use them, clear this information from their accounts, and turn off our ability to store it associated with their accounts going forward.

22. Facebook announced on April 4, 2018, it was making changes to the company's terms of service and its data policy and seeking input from users about those changes. Has the comment period for those changes closed? If Facebook gets feedback that users do not understand these changes, what will you do? Will you reopen the public comment period? What notice will consumers have before changes to the terms and conditions go into effect? Will consumers have the option to continue to use the previous version of Facebook instead of the updated version?

In April, we announced updates to our Data Policy and Terms of Service to better spell out what data we collect and how we use it in Facebook, Instagram, Messenger and other products, and also to explain the services we offer in language that is easier to understand. These updates are about making things clearer. We are not asking for new rights to collect, use or share user data on Facebook. After this announcement, we solicited feedback from our users for seven days. Following the comment period, we finalized and published these documents.

As we recently announced, we are showing everyone on Facebook an alert in their News Feed asking them to review important information about privacy, including the updates to our terms of service and Data Policy that we announced in April.

With regard to our Data Policy specifically, it has been available in a single webpage for many years. We recently updated our Data Policy in response to feedback that, among other things, we should provide more detailed explanations and improve the design of the policy. Like its predecessor, this policy is framed around short, easy-to-understand topics and questions, like "What kinds of information do we collect" and "How can I manage or delete information about me."

In designing both our newly updated Data Policy and its predecessor, as well as our Privacy Basics educational center, we were mindful of guidance from the FTC and many other experts that recommend so-called "layered" privacy policies, which make it easy to find topics and high-level information but enable people to access more detailed information if they wish to do so.

For more information, see Response to Question 9.

23. In congressional testimony, you indicated "[t]here will always be a version of Facebook that is free," signaling the company will continue to depend on advertising that requires users' personal information. Please explain why limiting personalized or targeted advertising could negatively impact consumers?

To build a secure product with extensive infrastructure that connects people across continents and cultures, we need to make sure everyone can afford it. To do this, we sell advertising, and we could not offer our service for free without selling advertising. Advertising lets us keep Facebook free, which ensures it remains affordable for everyone.

Separately, our core service involves personalizing all content, features, and recommendations that people see on Facebook services. No two people have the same experience on Facebook or Instagram, and they come to our services because they expect everything they see to be relevant to them. If we were not able to personalize or select ads or other content based on relevance, this would fundamentally change the service we offer on Facebook—and it would no longer be Facebook.

24. In a March 21, 2018 Facebook post, you stated that Facebook will ban any developer from the Facebook's Platform that does not agree to a full audit or that has misused personally identifiable information.

a. To date, have you identified any developers that will not agree to the audit? Please identify.

While our investigation is ongoing, as we have made clear, apps that refuse to agree to an audit will be banned from Facebook.

b. To date, have you identified any developers that misused personally identifiable information? Please identify.

Our investigation is in full swing, and we have large teams of internal and external experts working hard to investigate these apps as quickly as possible. As of early June 2018, thousands of apps have been investigated and around 200 apps have been suspended—pending a thorough investigation into whether they did in fact misuse any data. Where we find evidence that these or other apps did misuse data, we will ban them and let people know.

c. Please provide a timeline for when you expect to have this information. Will Facebook commit to sharing that information with the Committee and the public? If not, why not?

See Response to Question 7.

25. In a March 21, 2018 Facebook post, you stated that Facebook wants to ensure users understand which apps are collecting their information. What does this mean for a typical user? Will their user interface change? If so, when can we expect to see these changes? What metric will Facebook use to determine if users understand?

We will encourage people to manage the apps they use. We already show people what apps their accounts are connected to and allow them to control what data they've permitted those apps to use. But we're making it easier for people to see what apps they use and the information they have shared with those apps.

In general, improving people's understanding of how digital services work is an industry-wide challenge that we are highly committed to addressing. That's why, over the last 18 months, we've run a global series of design workshops called "Design Jams," bringing together experts in design, privacy, law and computer science to work collaboratively on new and innovative approaches. These workshops have run in Paris, London, Dublin, Berlin, Sao Paolo, Hong Kong and other cities, and included global regulators and policymakers. At these workshops, expert teams use "people centric design" methods to create innovative new design prototypes and experiences to improve transparency and education in digital services. These workshops inform Facebook's constantly-improving approach.

In recognition of the need for improved approaches to data transparency across all digital services, working with partners from academia, design and industry we recently launched TTC Labs, a design innovation lab that seeks to improve user experiences around personal data. TTC Labs is an open platform for sharing and innovation and contains insights from leading experts in academia, design and law, in addition to prototype designs from the Design Jams, template services and open-source toolkits for people-centric design for transparency, trust and control of data. Working collaboratively, and based on open-source approaches, TTC Labs seeks to pioneer new and more people-centric best practices for people to understand how their data is used by digital services, in ways that they find easy to understand and control.

Facebook is highly committed to improving people's experience of its own services as well as investing in new innovations and approaches to support improvements across the industry.

26. Once Facebook has allowed a third-party to access user data and that third-party pulls that data off the platform is there any way for Facebook to get that data back?

a. Is it fair for Facebook to promise users that Facebook protects their data when Facebook has no way to control what is done with data once it leaves the Facebook domain?

We are in the process of investigating every app that had access to a large amount of information before we changed our Platform in 2014. The investigation process is in full swing, and it has two phases. First, a comprehensive review to identify every app that had access to this amount of Facebook data and to focus on apps that present reason for deeper investigation. And second, where we have concerns, we will conduct interviews, make requests for information

(RFI)—which ask a series of detailed questions about the app and the data it has access to—and perform audits using expert firms that may include on-site inspections. We have large teams of internal and external experts working hard to investigate these apps as quickly as possible. As of early June 2018, thousands of apps have been investigated and around 200 apps have been suspended—pending a thorough investigation into whether they did in fact misuse any data. Where we find evidence that these or other apps did misuse data, we will ban them and let people know.

27. What is Facebook doing moving forward to ensure that it is protecting user information?

We've heard loud and clear that it's important to make privacy information and controls easy for people to find and use. We've made recent improvements to our privacy settings to centralize people's choices, and are providing access to people's key privacy choices through an updated Privacy Shortcuts feature.

With regard to our Data Policy specifically, it has been available in a single webpage for many years. We recently updated our Data Policy in response to feedback that, among other things, we should provide more detailed explanations and improve the design of the policy. Like its predecessor, this policy is framed around short, easy-to-understand topics and questions, like "What kinds of information do we collect" and "How can I manage or delete information about me."

Moreover, in April 2014, we announced that we would more tightly restrict our platform APIs to prevent abuse. At that time, we made clear that existing apps would have a year to transition—at which point they would be forced (1) to migrate to the more restricted API and (2) be subject to Facebook's new review and approval protocols. The vast majority of companies were required to make the changes by May 2015; a small number of companies (fewer than 100) were given a one-time extension of less than six months beyond May 2015 to come into compliance. (One company received an extension to January 2016.) In addition, in the context of our ongoing review of third-party apps, we discovered a very small number of companies (fewer than 10) that theoretically could have accessed limited friends' data as a result of API access that they received in the context of a beta test. We are not aware that any of this handful of companies used this access, and we have now revoked any technical capability they may have had to access any friends' data.

New apps that launched after April 30, 2014 were required to use our more restrictive platform APIs. We required apps seeking additional categories of data to undergo proactive review by our internal teams. We rejected more than half of the apps seeking these permissions, including the second version of Kogan's app.

We review apps to ensure that the requested permissions clearly improve the user experience and that the data obtained is tied to an experience within the app. We conduct a variety of manual and automated checks of applications on the platform for policy compliance, as well as random sampling. When we find evidence of or receive allegations of violations, we investigate and, where appropriate, employ a number of measures, including restricting

applications from our platform, preventing developers from building on our platform in the future, and taking legal action where appropriate.

Recently, we announced a number of additional steps we're taking to address concerns raised by Kogan's app.

- **Review our platform.** We will investigate all apps that had access to large amounts of data before the platform changes we announced in 2014, and we will audit any app where we identify suspicious activity. If we identify misuses of data, we'll take immediate action, including banning the app from our platform and pursuing legal action if appropriate.

- **Tell people about data misuse.** We will tell people about apps that have misused their data.

- **Turn off access for unused apps.** If someone has not used an app within the last three months, we will turn off the app's access to their data.

- **Restrict Facebook Login data.** We are changing Login, so that the only data that an app can request without app review will include name, profile photo, and email address. Requesting any other data will require approval from Facebook. We will also no longer allow apps to ask for access to information like religious or political views, relationship status and details, custom friends lists, education and work history, fitness activity, book reading and music listening activity, news reading, video watch activity, and games activity. We will encourage people to manage the apps they use. We already show people what apps their accounts are connected to and allow them to control what data they've permitted those apps to use. But we're making it easier for people to see what apps they use and the information they have shared with those apps.

- **Reward people who find vulnerabilities.** We launched the Data Abuse Bounty program so that people can report to us any misuses of data by app developers.

- **Update our policies.** We have updated our terms and Data Policy to explain how we use data and how data is shared with app developers.

28. Please provide an accounting of the number of fake accounts, organizations, or content that Facebook has deleted from the platform from 2007-2016.

We recently released enforcement statistics in our Community Standards Enforcement Report, including how many Facebook accounts we took action on because we determined they were fake. We will refine our approach over time, and we also hope to release additional metrics in future reports. The report is available at https://transparency.facebook.com/community-standards-enforcement.

29. Please describe in detail the steps Facebook has taken to combat the sale of counterfeit, substandard and falsified medicines sold through illegal online pharmacies.

We have an iterative process to help prevent opportunities for—and respond quickly to—attempts to sell illicit drugs on our platforms.

Our Community Standards and other policies make it very clear that buying, selling or trading non-medical or pharmaceutical drugs is not allowed on Facebook. Any time we become aware of content on Facebook that is facilitating activity like illicit drug sales, we remove it and have taken measures to minimize the opportunity for these activities to take place on our platform.

We make it easy for people to report any piece of content on Facebook—profiles, Pages, Groups, individual content and even comments.

If we identify violating content, we are able to look for associated profiles, Pages, groups, and accounts and remove them.

We have also made it harder for people to find content that facilitates the sale of opioids on our platform.

- We have removed content that violated our policies that was surfaced in Search.
- We have filtered the search results for hundreds of terms associated with drug sales in an effort to only return links to news and non-violating information about drugs that is shared on Facebook.
- We have removed thousands of terms from being suggested in search—meaning that our systems won't recognize the beginning of the word as it is being typed and suggest what the completed term to search is.

We continue to look for ways to get faster at finding and removing this content, working across our policy, operations, product, and partnerships teams. We also update our detection methods as bad actors work to game the system and bypass our safeguards.

30. Please provide an accounting of the opioid-related pages, events or content that facilitate the sale of illegal drugs that Facebook has removed from the service since the April 11, 2018 hearing.

We have worked for over a year on determining the methodology to measure our actions in enforcing our Community Standards and publishing the metrics that measure how effective we are at enforcing our policies.

Last month, for the first time, we shared the data we use internally to measure our effectiveness. At that time we shared metrics on our enforcement efforts between October 2017 – March 2018 on six policy areas: graphic violence, adult nudity and sexual activity, terrorist propaganda, hate speech, spam, and fake accounts. More details can be found in our Community

Standards Enforcement report at: https://transparency.facebook.com/community-standards-enforcement.

As we stated at the time, this is a work in progress and we will likely change our methodology over time as we learn more about how best to measure these metrics. We are also working to share metrics on additional policy areas over time.

The report is an attempt to open up about our removal of bad content from our site and make it easy for scholars, policymakers and community groups to give us feedback so that we can do better over time. While we can't change the fact that people will always try to post bad things—we can try to control how many times content that violates our Community Standards is seen. We know that measurement done right helps organizations make smart decisions about the choices they face—rather than simply relying on anecdote or intuition.

As we work to have metrics similar to those asked here, we continue to enforce our Community Standards. See Response to Question 29 for more detail.

31. Please describe in detail the steps Facebook has taken to ban the use of opioid or illegal drug terms within the Facebook search function.

We use a combination of technology and human review to inform Search rankings and we are working to improve our systems to filter from Search instances of illegal drug sales on Facebook.

We've taken a number of steps to minimize opportunities for illegal and policy-violating drug sales on Facebook. See Response to Question 29 for more detail.

We will continue to update our list of blocked terms as we learn of new terms bad actors may start adopting to avoid detection of their illicit activities.

We are committed to finding more ways to improve our efforts to combat the sale of illegal drugs on Facebook and we will continue to prioritize the issue this year. We recently launched a new feature on Facebook so that now, when people search for help with opioid misuse—as well as attempt to buy opioids—they are prompted with content at the top of the search results page that will ask them if they would like help finding free and confidential treatment referrals. This will then direct them to the Substance Abuse and Mental Health Services Administration National Helpline. The same resources will be available on Instagram in the coming weeks. This is one of a number of ways we are helping connect people with resources and communities to support them.

The Honorable Fred Upton

1. Does Facebook store a record of every time a Facebook user or non-user visits a website with an embedded Facebook pixel or social plug-in? Is that information part of the user's Facebook profile that Facebook uses to target ads to its users on behalf of marketers and campaigns?

Websites and apps choose whether they use Facebook services to make their content and ads more engaging and relevant and whether they share browser data or other information with Facebook or other companies when people visit their sites. These services include:

- Social plugins, such as our Like and Share buttons, which make other sites more social and help people share content on Facebook;
- Facebook Login, which lets people use their Facebook account to log into another website or app;
- Facebook Analytics, which helps websites and apps better understand how people use their services; and
- Facebook ads and measurement tools, which enable websites and apps to show ads from Facebook advertisers, to run their own ads on Facebook or elsewhere, and to understand the effectiveness of their ads.

Many companies offer these types of services and, like Facebook, they also get information from the apps and sites that use them. Twitter, Pinterest, and LinkedIn all have similar Like and Share buttons to help people share things on their services. Google has a popular analytics service. And Amazon, Google, and Twitter all offer login features. These companies—and many others—also offer advertising services. In fact, most websites and apps send the same information to multiple companies each time users visit them.

For example, when a user visits a website, their browser (for example Chrome, Safari or Firefox) sends a request to the site's server. The browser shares a user's IP address, so the website knows where on the internet to send the site content. The website also gets information about the browser and operating system (for example Android or Windows) they're using because not all browsers and devices support the same features. It also gets cookies, which are identifiers that websites use to know if a user has visited before.

A website typically sends two things back to a user's browser: first, content from that site; and second, instructions for the browser to send the user's request to the other companies providing content or services on the site. So, when a website uses one of our services, our users' browsers send the same kinds of information to Facebook as the website receives. We also get information about which website or app our users are using, which is necessary to know when to provide our tools.

In addition, we also enable ad targeting options—called "interests" and "behaviors"—that are based on people's activities on Facebook, and when, where, and how they connect to the internet (such as the kind of device they use and their mobile carrier). These options do not

reflect people's personal characteristics, but we still take precautions to limit the potential for advertisers to misuse them.

We do not use web browsing data to show ads to non-users or otherwise store profiles about non-users. Our goal is to show people content (including advertising) that is relevant to their interests. We use information people have provided on Facebook—such as things they've liked or posts they've engaged with—to help determine what people will be interested in. Like most online advertising companies, we also inform our judgments about what ads to show based on apps and websites that people use off of Facebook. People can turn off our use of web browser data and other data from third-party partners to show them ads through a control in Ads Preferences. They can also customize their advertising experience by removing interests that they do not want to inform the Facebook ads they see. In addition, a person's browser or device may offer settings that allow users to choose whether browser cookies are set and to delete them.

The Honorable John Shimkus

1. **Facebook's Ad Manager tool has reportedly been used by casinos to target children aged 13-17 whom they believe are interested in online gambling. Although these ads may be appropriate for adults, what is Facebook doing to ensure children and their private information are protected from threats posed by aggressive and sometimes unscrupulous advertisers?**

We take the privacy, safety, and security of all those who use our platform very seriously, and when it comes to minors (13 to 18 years old), we provide special protections and resources.

We provide special protections for teens on Facebook and Messenger. We provide education before allowing teens to post publicly. We don't show search results based on specific profile data (high school, birthday/age, and hometown, or current city) of teens to unconnected adults when the adults search on Facebook. Unconnected adults can't message minors who are 13-17. And, we prohibit search engines off Facebook from indexing minors' profiles. And, we have age limits for advertisements. For example, ads for dating sites, financial services, and other products or services are gated to users under 18.

We provide special resources to help ensure that they enjoy a safe and secure experience. For example, we recently announced the launch of our Youth Portal, which is available in 60 languages at https://www.facebook.com/safety/youth. This portal is a central place for teens that includes:

- **Education.** Information on how to get the most out of products like Pages, Groups, Events, and Profile, while staying safe. Plus, information on the types of data Facebook collects and how we use it.

- **Peer Voices.** First-person accounts from teens around the world about how they are using technology in new and creative ways.

- **Ways to control user experience.** Tips on things like security, reporting content, and deciding who can see what teens share.

- **Advice.** Guidelines for how to safely get the most out of the internet.

Instagram also will be providing information to teens to show them where they can learn about all of the tools on Instagram to manage their privacy and stay safe online, including how to use the new Access and Download tools to understand what they have shared online and learn how to delete things they no longer want to share. We are also making this information available in formats specifically designed for young users, including video tutorials for our privacy and safety tools, and teen-friendly FAQs about the Instagram Terms of Use, Data Policy, safety features, and Community Guidelines.

Instagram has also launched new content on Instagram Together, including videos and FAQs about privacy controls; information on how to use safety features, including comment controls, blocking accounts, reporting abuse, spam, or troubling messages; information on responsible social media use; and FAQs about safety on Instagram. We will be reaching out to

users under 18 on Instagram to encourage them to learn more on Instagram Together, available at https://www.instagram-together.com/.

Further, we have content restrictions and reporting features for everyone, including minors. We have Community Standards that prohibit hate speech, bullying, intimidation, and other kinds of harmful behavior. We encourage people to report posts and rely on our team of content reviewers around the world to review reported content. Our reviewers are trained to look for violations and enforce our policies consistently and as objectively as possible. When reviewed by our team, we hide certain graphic content from users under 18 (and include a warning for adults). We are also working to improve our ability to get our community help in real time, especially in instances where someone is expressing thoughts of suicide or self-harm, by expanding our use of proactive detection, working with safety experts and first-responders, and dedicating more reviewers from our Community Operations team.

We also built a messaging app for children 12 and under to connect with their friends and family and that must be created by an established adult Facebook account holder for their child and this is controlled by the parent from the parents' Facebook account. We have no plans to monetize Messenger Kids, and monetization was not what motivated us to build it. Moreover, there are no in-app purchases, and we do not use the data in Messenger Kids to advertise to kids or their parents. In developing the app, we assembled a committee of advisors, including experts in child development, online safety, and media and children's health, and we continue to work with them on an ongoing basis. In addition, we conducted roundtables with parents from around the country to ensure we were addressing their concerns and built the controls they need and want in the app. We are committed to approaching all efforts related to children 12 and under thoughtfully, and with the guidance and input of experts and parents.

We do not automatically create a Facebook account for Messenger Kids users, or automatically transition a Messenger Kids account into a Facebook account once a child turns 13. However, when someone becomes 13, they can create a Facebook and Messenger account. We may eventually provide a way for the person to transition their message threads from Messenger Kids into Messenger to keep the conversations if they want them. We have no plans to use this data for ads.

The Honorable Michael C. Burgess

1. As part of the 2011 consent decree, Facebook is required to provide privacy audits every two years to the FTC. It is my understanding that Facebook is also conducting audits of applications that had or have access to large amounts of data and will bring in third-party auditors to investigate any suspicious activity.

a. Are these two audit efforts independent of each other?

As part of the 2011 consent decree, Facebook is required to have an independent assessor perform an examination of its privacy program. To date, three assessments have been completed and submitted to the FTC: a 180-Day assessment report (dated April 16, 2013), a biennial report covering the period between February 12, 2013 and February 11, 2015 (dated April 13, 2015), and a biennial report covering the period between February 12, 2015 and February 11, 2017 (dated April 12, 2017). These assessments were completed prior to the company's announcement of its investigation of third-party apps with access to a significant amount of user data before 2014. We note that Facebook evaluates and adjusts its privacy program in light of the results of its monitoring activities, any material changes to its operations or business arrangements, or any other circumstances that it knows or has reason to know may have a material impact on the effectiveness of its privacy program.

b. Is any of the information from Facebook's application audits also being shared with the FTC to comply with the consent decree?

The Consent Order does not require ongoing reporting obligations of the type asked in this question. We note that we regularly engage in dialogue with the FTC, and we are providing to the public information about the audit being performed by Facebook as described in your question.

2. You stated during questioning that you believe the improper release of user information to Cambridge Analytica did not violate the 2011 consent decree. Please explain how the Cambridge Analytica incident did not violate the consent decree.

We furnished extensive information to the FTC regarding the ability for users to port their Facebook data (including friends data that had been shared with them) with apps on Facebook's platform, as part of the FTC's investigation culminating in the July 27, 2012 Consent Order. The Consent Order memorializes the agreement between Facebook and the FTC and did not require Facebook to turn off the ability for people to port friends data that had been shared with them on Facebook to apps they used. Facebook voluntarily changed this feature of the Platform in 2014, however.

Among other things, the Consent Order obligates Facebook not to misrepresent the extent to which it maintains the privacy or security of covered information (Section I), not to materially exceed the restrictions of a privacy setting that applies to nonpublic user information without affirmative express consent (Section II), and to implement a comprehensive privacy program that is subjected to ongoing review by an independent assessor (Sections IV and V). Facebook accurately represented the operation of its developer Platform and the circumstances under which people could share data (including friends data) with developers, honored the restrictions of all

privacy settings that covered developer access to data, and implemented a comprehensive privacy program built on industry-leading controls and principles, which has undergone ongoing review by an independent assessor approved by the FTC.

3. Many consumers do not read or understand the Facebook's policies and terms and conditions they agree to in order to access an application or service.

a. If a consumer took the time to thoroughly evaluate terms and conditions, what elements of your policies and terms and services indicate strong consumer protections? What elements should a consumer recognize that indicate weak protections?

Privacy is at the core of everything we do, and our approach to privacy starts with our commitment to transparency and control. Our threefold approach to transparency includes, first, whenever possible, providing information on the data we collect and use and how people can control it in context and in our products. Second, we provide information about how we collect and use data in our user agreements and related educational materials. And third, we enable people to learn more about the specific data we have about them through interactive tools such as Download Your Information, which lets people download a file containing data that they may want to take to another service, and Access Your Information, a tool we are launching that will let people more easily access and manage their data on Facebook.

Our approach to control is based on the belief that people should be able to choose who can see what they share and how their data shapes their experience on Facebook. People can control the audience for their posts and the apps that can receive their data. They can see and delete the history of their activities on Facebook, and, if they no longer want to use Facebook, they can delete their account and the data associated with it. Of course, we recognize that controls are only useful if people know how to find and use them. That is why we continuously deliver in-product educational videos in people's News Feeds on important privacy topics. We are also inviting people to take our Privacy Checkup—which prompts people to review key data controls—and we are sharing privacy tips in education campaigns off of Facebook, including through ads on other websites. To make our privacy controls easier to find, we are launching a new settings menu that features core privacy settings in a single place. We are always working to help people understand and control how their data shapes their experience on Facebook.

b. Do you have any metrics on, or can you measure, how many users access Facebook's terms and conditions?

We believe that it's important to communicate with people about the information that we collect and how people can control it. This is why we work hard to provide this information to people in a variety of ways: in our Data Policy, and in Privacy Basics, which provides walkthroughs of the most common privacy questions we receive. Beyond simply disclosing our practices, we also think it's important to give people access to their own information, which we do through our Download Your Information and Access Your Information tools, Activity Log, and Ad Preferences, all of which are accessible through our Privacy Shortcuts tool. We also provide information about these topics as people are using the Facebook service itself.

As to your specific question, there is no single number that measures how much time people spend understanding how Facebook services work, in large part because Facebook seeks, as much as possible, to put controls and information in context within its service. While "up front" information like that contained in the terms of service are useful, research overwhelmingly demonstrates that in-product controls and education are the most meaningful to people and the most likely to be read and understood. On-demand controls are also important, and we recently redesigned our entire settings menu on mobile devices from top to bottom to make things easier to find. We also created a new Privacy Shortcuts, a menu where people can control their data in just a few taps, with clearer explanations of how our controls work. The experience is now clearer, more visual, and easy-to-find.

Improving people's understanding of how digital services work is an industry-wide challenge that we are highly committed to addressing. That's why, over the last 18 months, we've run a global series of design workshops called "Design Jams", bringing together experts in design, privacy, law, and computer science to work collaboratively on new and innovative approaches. These workshops have run in Paris, London, Dublin, Berlin, Sao Paolo, Hong Kong, and other cities, and included global regulators and policymakers. At these workshops, expert teams use "people centric design" methods to create innovative new design prototypes and experiences to improve transparency and education in digital services. These workshops inform Facebook's constantly-improving approach.

In recognition of the need for improved approaches to data transparency across all digital services, working with partners from academia, design, and industry we recently launched TTC Labs, a design innovation lab that seeks to improve user experiences around personal data. TTC Labs is an open platform for sharing and innovation and contains insights from leading experts in academia, design, and law, in addition to prototype designs from the design jams, template services and open-source toolkits for people-centric design for transparency, trust and control of data. Working collaboratively, and based on open-source approaches, TTC Labs seeks to pioneer new and more people-centric best practices for people to understand how their data is used by digital services, in ways that they find easy to understand and control.

Facebook is highly committed to improving people's experience of its own services as well as investing in new innovations and approaches to support improvements across the industry.

4. On January 11, 2018, you posted that Facebook had started making changes to its algorithm to better tailor content to users based on preferences and interactions with a user's closest 'friends'. You described this change as promoting "news that is trustworthy, informative, and local."

a. Can you describe how the algorithm determines which content is "trustworthy, informative, and local?" In your description, please delineate what specific data is input into the algorithm to determine which content is "trustworthy, informative, and local".

At Facebook, we define false news as "[n]ews articles that purport to be factual, but which contain intentional misstatements of fact with the intention to arouse passions, attract viewership, or deceive."

We believe that tech companies, media companies, newsrooms, and educators all need to work together to address this societal problem. We are engaged with partners across these industries to help create a more informed community.

We are working to build a more informed community by promoting trustworthy, informative, and local news and by focusing on four different strategies to address misinformation:

- Strengthening enforcement of our authenticity policies. We are investing heavily in new technology and hiring thousands more people to tackle the problem of inauthenticity on the platform. Fake accounts are often associated with false news, so this is an area that will have a huge impact on curbing the spread of inaccurate information.

- Finding industry solutions. All of us—from tech companies and media companies to newsrooms and classrooms—must work together to find industry solutions to strengthen the online news ecosystem and our own digital literacy. That's why we're collaborating with others who operate in this space. Last January, we announced The Facebook Journalism Project, an initiative that seeks to establish stronger ties between Facebook and the news industry. The project is focused on developing news products, providing training and tools for journalists, and working with publishers and educators on how we can equip people with the knowledge they need to be informed readers in the digital age. Since launching the Journalism Project, we've met with more than 2,600 publishers around the world to understand how they use our products and how we can make improvements to better support their needs.

- Disrupting economic incentives. When it comes to fighting false news, we've found that a lot of it is financially motivated. So, one of the most effective approaches is removing the economic incentives for those who traffic in inaccurate information. We've done things like block ads from pages that repeatedly share false news and significantly limit the distribution of web pages that deliver low quality web experiences.

- Building new products. We believe it's important to amplify the good effects of social media and mitigate the bad—to contribute to the diversity of ideas, information, and view points, while strengthening our common understanding.

    - We believe giving people more context can help them decide what to trust and what to share. The third-party fact-checking program we have developed uses reports from our community, along with other signals, to send stories to accredited third-party fact checking organizations. If the fact-checking organizations identify a story as fake, we will suggest related articles in News Feed to show people different points of view, including information from fact

checkers. Stories that have been disputed may also appear lower in News Feed. Our own data analytics show that a false rating from one of our fact checking partners reduces future impressions on Facebook by 80 percent.

- We're also testing Article Context as a way of giving people more information about the material they're reading on Facebook. Since we launched this test, some of the articles people see in News Feed will feature an "i" icon that allows them to access more information at the tap of a button. The information we surface is pulled from across the internet, and includes things like the publisher's Wikipedia entry, trending articles or related articles about the topic, and information about how the article is being shared on Facebook. In some cases, if that information is unavailable, we will let people know since that can also be helpful context.

5. Apparently, Facebook's algorithm change may have resulted in intentional or unintentional censoring of certain types of information and news. As indication of such, some conservative pages, like Diamond and Silk, have been deemed "unsafe to the community." Previously, certain Facebook features allowed users and advertisers to manipulate how information and news was posted. An example of this was reported by Eric Wilson when a Facebook page opposing his campaign candidate misrepresented the title and intent of a Washington Post article.

a. All of these instances lead many to believe that Facebook tailors its products and services based on political agenda? Is this true?

Being a platform for all ideas is a foundational principle of Facebook. We are committed to ensuring there is no bias in the work we do.

Suppressing content on the basis of political viewpoint or preventing people from seeing what matters most to them is directly contrary to Facebook's mission and our business objectives.

For example, when allegations of political bias surfaced in relation to Facebook's Trending Topics feature, we immediately launched an investigation to determine if anyone violated the integrity of the feature or acted in ways that are inconsistent with Facebook's policies and mission. We spoke with current reviewers and their supervisors, as well as a cross-section of former reviewers; spoke with our contractor; reviewed our guidelines, training, and practices; examined the effectiveness of operational oversight designed to identify and correct mistakes and abuse; and analyzed data on the implementation of our guidelines by reviewers.

Ultimately, our investigation revealed no evidence of systematic political bias in the selection or prominence of stories included in the Trending Topics feature. In fact, our analysis indicated that the rates of approval of conservative and liberal topics are virtually identical in Trending Topics. Moreover, we were unable to substantiate any of the specific allegations of politically-motivated suppression of subjects or sources, as reported in the media. To the contrary, we confirmed that most of those subjects were in fact included as trending topics on multiple occasions, on dates and at intervals that would be expected given the volume of discussion around those topics on those dates.

Nonetheless, as part of our commitment to continually improve our products and to minimize risks where human judgment is involved, we are making a number of changes:

- We have engaged an outside advisor, former Senator Jon Kyl, to advise the company on potential bias against conservative voices. We believe this external feedback will help us improve over time and ensure we can most effectively serve our diverse community and build trust in Facebook as a platform for all ideas.

- We continue to expand our list of outside partner organizations to ensure we receive feedback on our content policies from a diverse set of viewpoints.

- We have made our detailed reviewer guidelines public to help people understand how and why we make decisions about the content that is and is not allowed on Facebook.

- We have launched an appeals process to enable people to contest content decisions with which they disagree.

- We are instituting additional controls and oversight around the review team, including robust escalation procedures and updated reviewer training materials.

These improvements and safeguards are designed to ensure that Facebook remains a platform for all ideas and enables the broadest spectrum of free expression possible.

As to Diamond and Silk, we mishandled communication with Diamond and Silk for months. Their frustration was understandable, and we apologized to them. The message they received on April 5, 2018 that characterized their Page as "dangerous" was incorrect and not reflective of the way we seek to communicate with our community and the people who run Pages on our platform.

6. According to the timeline you posted on your page, Facebook learned of the misuse of user data by an application associated with Cambridge Analytica in 2015. You claim that you banned the application and asked that Cambridge Analytica remove all improperly obtained data, but you did not immediately notify potentially affected users.

a. What if, because of this or other breaches, a user's identity is stolen. Do you have a plan in place to help those users recover?

Facebook is generally open to the idea of breach notification requirements, particularly legislation that would centralize reporting and ensure a consistent approach across the United States. For example, in Europe, the GDPR requires notification to a lead supervisory authority, rather than individual member states, in cases of a data breach. In the United States, however, there is no centralized notification scheme, and instead, reporting obligations vary widely across all 50 states. This complexity makes it harder to respond appropriately and swiftly to protect people in the event of a data breach. We believe this is an important issue and an area that is ripe for thoughtful regulation.

When Facebook learned about Kogan's breach of Facebook's data use policies in December 2015, it took immediate action. The company retained an outside firm to assist in investigating Kogan's actions, to demand that Kogan and each party he had shared data with delete the data and any derivatives of the data, and to obtain certifications that they had done so. Because Kogan's app could no longer obtain access to most categories of data due to changes in Facebook's platform, the company's highest priority at that time was ensuring deletion of the data that Kogan may have accessed before these changes took place. With the benefit of hindsight, we wish we had notified people whose information may have been impacted. Facebook has since notified all people potentially impacted with a detailed notice at the top of their News Feed.

b. Do you have or will you put in place policies to alert users of data breaches within a reasonable timeframe? If not, why not?

Facebook monitors its systems for potential breaches of personal data and logs any potential breach in a system that automatically triggers expedited review. Facebook reviews such potential incidents to determine: (i) whether there was in fact an incident; (ii) its root cause, including short- and long-term remediation (if applicable); and (iii) our legal and ethical obligations. Facebook moves quickly to review potential incidents. Because of the fluid nature of an incident, there are no set timelines for completion of reviews and addressing a discovered vulnerability, but any potential breach is escalated for high priority processing. Facebook notifies users in accordance with its obligations under applicable law and has also notified people in cases where there was no legal obligation to do so but we nevertheless determined it was the right thing to do under the circumstances.

c. Would you support data breach notification legislation?

See Response to Question 6(a).

The Honorable Marsha Blackburn

1. Can you please describe your history and relationship with Fight For the Future?

a. Please address this from a personal, corporate, and employee standpoint.

Facebook is not affiliated with Fight for the Future and does not provide financial support to the organization. In one instance to date, Facebook made a $5 contribution to Fight for the Future through its pilot matching program for non-profit birthday fundraisers. Under this program, when Facebook users create birthday fundraisers to support causes they care about, eligible non-profits with 501(c)(3) status could receive a $1, $2, or a $5 matching donation from Facebook. Between May 24 and June 25, 2018, over 18,000 organizations received some amount of matching funds from Facebook. To date, the top three non-profits in donations received through Facebook's matching program are St. Jude's Children's Research Hospital, the American Cancer Society, and the Wounded Warrior project.

2. During our exchange at the April 11, 2018 hearing, I recommended that you and your team refresh your memory regarding my privacy legislation - the BROWSER Act. Instead of simply asking for a "commitment" to work together on this effort -I have two specific follow-up requests:

a. Please have your team provide feedback on specific provisions of the BROWSER Act.

b. As part of this commitment - will Facebook commit to not spending money to weaken privacy legislation - both on the state and federal level? This would include outside groups that Facebook is a member of, such as the Internet Association.

Facebook is generally not opposed to regulation but wants to ensure it is the right regulation. The issues facing the industry are complex, multi-faceted, and affect an important part of peoples' lives. As such Facebook is absolutely committed to working with policymakers, like Congress, to craft the right regulations. As requested, we will follow up with your staff to provide specific feedback on the BROWSER Act.

The Honorable Steve Scalise

1. During your testimony at the joint Senate Commerce and Judiciary Committee hearing on April 10, 2018, were asked about Facebook's ability to track users' activity across various devices after they have logged off Facebook, and whether Facebook could follow users' browser histories when they were not on the social network. During your testimony the next day, you tried to clarify how this data is collected, and for what purpose. In doing so, you stated that one of the reasons for data collection is for security purposes.

a. Is the data Facebook collects for security purposes also used as part of Facebook's ad-based business model?

When people visit apps or websites that feature our technologies—like the Facebook Like or Comment button—our servers automatically log (i) standard browser or app records of the fact that a particular device or user visited the website or app (this connection to Facebook's servers occurs automatically when a person visits a website or app that contains our technologies, such as a Like button, and is an inherent function of internet design); and (ii) any additional information the publisher of the app or website chooses to share with Facebook about the person's activities on that site (such as the fact that a purchase was made on the site). This is a standard feature of the internet, and most websites and apps share this same information with multiple different third-parties whenever people visit their website or app. For example, the House Energy and Commerce Committee's website shares information with Google Analytics to help improve the site. This means that, when a person visits the Committee's website, it sends browser information about their visit to that third party. More information about how this works is available at https://newsroom.fb.com/news/2018/04/data-off-facebook/.

Our Data Policy describes in detail what we do with the information we receive. There are three main ways in which Facebook uses the information we get from other websites and apps: providing our services to these sites or apps; improving safety and security on Facebook; and enhancing our own products and services.

- Providing Our Services

    - *Social plugins and Facebook Login.* We use a person's IP address, browser/operating system information, and the address of the website or app they are using to make these features work. For example, knowing the IP address allows us to send the Like button to the person's browser and helps us show it in the person's language. Cookies and device identifiers help us determine whether the person is logged in, which makes it easier to share content or use Facebook to log into another app.

    - *Facebook Analytics.* Facebook Analytics (https://analytics.facebook.com/) gives websites and apps data about how they are used. IP addresses help us list the countries where people are using an app. Browser and operating system information enable us to give developers information about the platforms people use to access their app. Cookies and other identifiers help us

count the number of unique visitors. Cookies also help us recognize which visitors are Facebook users so we can provide aggregated demographic information, like age and gender, about the people using the app.

- *Ads.* Facebook Audience Network enables other websites and apps to show ads from Facebook advertisers. When we get a request to show an Audience Network ad, we need to know where to send it and the browser and operating system a person is using. Cookies and device identifiers help us determine whether the person uses Facebook. If they don't, we can show an ad encouraging them to sign up for Facebook. If they do, we'll show them ads from the same advertisers that are targeting them on Facebook. We can also use the fact that they visited a site or app to show them an ad from that business—or a similar one—back on Facebook.

- *Ad Measurement.* An advertiser can choose to add the Facebook Pixel, some computer code, to their site. This allows us to give advertisers stats about how many people are responding to their ads—even if they saw the ad on a different device—without us sharing anyone's personal information.

- Keeping Your Information Secure

  - We also use the information we receive from websites and apps to help protect the security of Facebook. For example, receiving data about the sites a particular browser has visited can help us identify bad actors. If someone tries to log into an account using an IP address from a different country, we might ask some questions to verify it's the right person. Or if a browser has visited hundreds of sites in the last five minutes, that's a sign the device might be a bot. We'll ask them to prove they're a real person by completing additional security checks.

- Improving Our Products and Services

  - The information we receive also helps us improve the content and ads we show on Facebook. So if a person visits a lot of sports sites that use our services, you might see sports-related stories higher up in your News Feed. If you've looked at travel sites, we can show you ads for hotels and rental cars.

2. At the April 11, 2018 hearing, you testified that there is no directive to include bias in your algorithms. However, there are examples that myself and others have pointed to that show otherwise.

a. Can you say with certainty that there has not been development of algorithms that have an intentional bias against conservative views by employees of your company? If you maintain that no bias is included, please explain why certain, legitimate content, such as that of Diamond and Silk, is restricted.

Being a platform for all ideas is a foundational principle of Facebook. We are committed to ensuring there is no bias in the work we do. Suppressing content on the basis of political

viewpoint or preventing people from seeing what matters most to them is directly contrary to Facebook's mission and our business objectives.

We are committed to free expression and err on the side of allowing content. When we make a mistake, we work to make it right. And we are committed to constantly improving our efforts so we make as few mistakes as humanly possible. Decisions about whether to remove content are based on whether the content violates our Community Standards. Discussing controversial topics or espousing a debated point of view is not at odds with our Community Standards, the policies that outline what is and isn't allowed on Facebook. We believe that such discussion is important in helping bridge division and promote greater understanding.

We mishandled communication with Diamond and Silk for months. Their frustration was understandable, and we apologized to them. The message they received on April 5, 2018 that characterized their Page as "dangerous" was incorrect and not reflective of the way we seek to communicate with our community and the people who run Pages on our platform.

As part of our commitment to continually improve our products and to minimize risks where human judgment is involved, we are making a number of changes:

- We have engaged an outside advisor, former Senator Jon Kyl, to advise the company on potential bias against conservative voices. We believe this external feedback will help us improve over time and ensure we can most effectively serve our diverse community and build trust in Facebook as a platform for all ideas.

- We continue to expand our list of outside partner organizations to ensure we receive feedback on our content policies from a diverse set of viewpoints.

- We have made our detailed reviewer guidelines public to help people understand how and why we make decisions about the content that is and is not allowed on Facebook.

- We have launched an appeals process to enable people to contest content decisions with which they disagree.

- We are instituting additional controls and oversight around the review team, including robust escalation procedures and updated reviewer training materials.

These improvements and safeguards are designed to ensure that Facebook remains a platform for all ideas and enables the broadest spectrum of free expression possible.

The Honorable Robert Latta

1. What policies, mechanisms or procedures were in place prior to November 2016 to verify whether Russian or Chinese authorities used data acquisition and sharing methods as other third parties, including Obama for America and Dr. Kogan, to scrape the entire Facebook Platform for their own gain? Please describe the policies, mechanisms, or procedures were put in place since 2016, as well as when they were implemented, to protect against nation-states from using similar techniques and methods.

In the run-up to the 2016 elections, we were focused on the kinds of cybersecurity attacks typically used by nation states, for example phishing and malware attacks. And we were too slow to spot this type of information operations interference. Since then, we've made important changes to prevent bad actors from using misinformation to undermine the democratic process.

Protecting a global community of more than 2 billion involves a wide range of teams and functions, and our expectation is that those teams will grow across the board. For example, we have dedicated information security and related engineering teams.

Protecting the security of information on Facebook is at the core of how we operate. Security is built into every Facebook product, and we have dedicated teams focused on each aspect of data security. From encryption protocols for data privacy to machine learning for threat detection, Facebook's network is protected by a combination of advanced automated systems and teams with expertise across a wide range of security fields. Our security protections are regularly evaluated and tested by our own internal security experts and independent third parties. For the past seven years, we have also run an open bug bounty program that encourages researchers from around the world to find and responsibly submit security issues to us so that we can fix them quickly and better protect the people who use our service.

We anticipate continuing to grow these teams by hiring a range of experts, including people with specific types of threat intelligence expertise.

This will never be a solved problem because we're up against determined, creative and well-funded adversaries. But we are making steady progress. Here is a list of the 10 most important changes we have made:

- **Ads transparency.** Advertising should be transparent: users should be able to see all the ads an advertiser is currently running on Facebook, Instagram and Messenger. And for ads with political content, we've created an archive that will hold ads with political content for seven years—including information about ad impressions and spend, as well as demographic data such as age, gender, and location. People in Canada and Ireland can already see all the ads that a Page is running on Facebook—and we just launched View Active Ads globally.

- **Verification and labeling.** Every advertiser will now need to confirm their ID and location before being able to run any ads with political content in the US. All ads with political content will also clearly state who paid for them.

- **Updating targeting.** We want ads on Facebook to be safe and civil. We thoroughly review the targeting criteria advertisers can use to ensure they are consistent with our principles. As a result, we removed nearly one-third of the targeting segments used by the IRA. We continue to allow some criteria that people may find controversial. But we do see businesses marketing things like historical books, documentaries or television shows using them in legitimate ways.

- **Better technology.** Over the past year, we've gotten increasingly better at finding and disabling fake accounts. We now block millions of fake accounts each day as people try to create them—and before they've done any harm. This is thanks to improvements in machine learning and artificial intelligence, which can proactively identify suspicious behavior at a scale that was not possible before—without needing to look at the content itself.

- **Action to tackle fake news.** We are working hard to stop the spread of false news. We work with third-party fact-checking organizations to limit the spread of articles rated false. To reduce the spread of false news, we remove fake accounts and disrupt economic incentives for traffickers of misinformation. We also use various signals, including feedback from our community, to identify potential false news. In countries where we have partnerships with independent third-party fact-checkers, stories rated as false by those fact-checkers are shown lower in News Feed. If Pages or domains repeatedly create or share misinformation, we significantly reduce their distribution and remove their advertising rights. We also want to empower people to decide for themselves what to read, trust, and share. We promote news literacy and work to inform people with more context. For example, if third-party fact-checkers write articles about a news story, we show them immediately below the story in the Related Articles unit. We also notify people and Page Admins if they try to share a story, or have shared one in the past, that's been determined to be false. In addition to our own efforts, we're learning from academics, scaling our partnerships with third-party fact-checkers and talking to other organizations about how we can work together.

- **Significant investments in security.** We're doubling the number of people working on safety and security from 10,000 last year to over 20,000 this year. We expect these investments to impact our profitability. But the safety of people using Facebook needs to come before profit.

- **Industry collaboration.** Recently, we joined 34 global tech and security companies in signing a TechAccord pact to help improve security for everyone.

- **Information sharing and reporting channels.** In the 2017 German elections, we worked closely with the authorities there, including the Federal Office for Information Security (BSI). This gave them a dedicated reporting channel for security issues related to the federal elections.

- **Tracking 40+ elections.** In recent months, we've started to deploy new tools and teams to proactively identify threats in the run-up to specific elections. We first

tested this effort during the Alabama Senate election, and plan to continue these efforts for elections around the globe, including the US midterms. Last year we used public service announcements to help inform people about fake news in 21 separate countries, including in advance of French, Kenyan and German elections.

- **Action against the Russia-based IRA.** In April, we removed 70 Facebook and 65 Instagram accounts—as well as 138 Facebook Pages—controlled by the IRA primarily targeted either at people living in Russia or Russian-speakers around the world including from neighboring countries like Azerbaijan, Uzbekistan, and Ukraine. The IRA has repeatedly used complex networks of inauthentic accounts to deceive and manipulate people in the US, Europe, and Russia—and we don't want them on Facebook anywhere in the world.

2. Facebook VP Andrew Bosworth previously highlighted concerns over serious misuse of the Facebook Platform. In a June 2016 memo, Mr. Bosworth goes as far to suggest that people may die as a result of your platform. Have concerns of misuse been raised to executive officers and/or board members, and what steps did they take address concerns of misuse seriously? Please describe.

Facebook recognizes that connecting people isn't enough by itself. We also need to work to bring people closer together. We changed our whole mission and company focus to reflect this last year.

3. According to numerous media reports, Facebook hired quantitative social psychologist Joseph Chancellor in November 2015, approximately two months after leaving as a founding director of Global Science Research (GSR). It is alleged that GSR was a third- party (along with Dr. Kogan, Cambridge Analytica and others) that may have inappropriately accessed and shared data and information of Facebook users, as well as a Friend of users.

a. What is Mr. Chancellor's employment relationship with Facebook? Is Mr. Chancellor still employed by the company, and if he is what is his title and role in the company? What are his job responsibilities? Have those changed since 2015?

Mr. Chancellor is a quantitative researcher on the User Experience Research team at Facebook, whose work focuses on aspects of virtual reality. We are investigating Mr. Chancellor's work with Kogan/GSR.

b. If Mr. Chancellor is no longer an employee of Facebook, is he serving in any advisory or consulting collecting any payroll or any cash or non-cash compensation from Facebook?

See Response to Question 3(a).

c. Is Mr. Chancellor subject to a confidentiality or non-disclosure agreement with Facebook?

All employees of Facebook (as with many businesses) are required to sign a standard confidentiality agreement as part of their employment, and Mr. Chancellor is no exception.

The Honorable David McKinley

1. Please list, in detail, the steps that Facebook is taking to combat Facebook being a platform for illegal online pharmacies to sell prescription opioids and other controlled substances (and counterfeit drugs) without a prescription?

We have an iterative process to help prevent opportunities for—and respond quickly to—illicit drug sales on our platforms. Our Community Standards and other policies make it very clear that buying, selling, or trading non-medical or pharmaceutical drugs is not allowed on Facebook. Any time we become aware of content on Facebook that is facilitating activity like illicit drug sales, we remove it and have taken measures to minimize the opportunity for these activities to take place on our platform.

We make it easy for people to report any piece of content on Facebook—profiles, Pages, Groups, individual content and even comments. If we identify violating content, we are able to look for associated profiles, Pages, groups, and accounts and remove them.

We have also made it harder for people to find content that facilitates the sale of opioids on our platform.

- We have removed content that violated our policies that was surfaced in Search.
- We have filtered the search results for hundreds of terms associated with drug sales in an effort to only return links to news and non-violating information about drugs that is shared on Facebook.
- We have removed thousands of terms from being suggested in search—meaning that our systems won't recognize the beginning of the word as it is being typed and suggest what the completed term to search is.

We continue to look for ways to get faster at finding and removing this content, working across our policy, operations, product, and partnerships teams. We also update our detection methods as bad actors work to game the system and bypass our safeguards.

2. In the hearing, I questioned Mr. Zuckerberg about specific listings of illegal prescription drugs and they were taken down momentarily. If I had not drawn attention to this issue, would someone have been as proactive in taking them down?

We remove content on Facebook that is facilitating the sale of illegal drugs once we are made aware of it. We make it easy for people to report any piece of content on —profiles, Pages, Groups, individual content and even comments. If we identify violating content, we are able to look for associated profiles, Pages, groups, and accounts and remove them.

We continue to look for ways to get faster at finding and removing this content, working across our policy, operations, product, and partnerships teams. We also update our detection methods as bad actors work to game the system. We encourage our community to continue to tell us if they see this behavior anywhere on our service.

Further, the organic content that was raised during the testimony was from months earlier and had already been removed from our site.

3. If Facebook has 20,000 employees working on security, how many are designated as full-time employees working to combat the sale of illegal drugs on the platform?

Our effort to make our platform safer and more secure is a holistic one that involves a continual evaluation of our personnel, processes, and policies, and we make changes as appropriate.

We are doubling the size of our security and content review teams (from 10,000 to 20,000) over the course of this year. We currently have approximately 15,000 people working on these teams. The team also includes specialists in areas like child safety, hate speech and counter-terrorism, software engineers to develop review systems, quality control managers, policy specialists, legal specialists, and general reviewers.

We employ a mix of full-time employees, contractors, and vendor partners to assist with content review and help us scale globally. Our content review team is global, reviews reports in over 50 languages, 24 hours a day, 7 days a week and the vast majority of reports are reviewed within 24 hours. Our goal is always to have the right number of skilled people with the right language capabilities to help ensure incoming reports are reviewed quickly and efficiently. We hire people with native language and other specialist skills according to the needs we see from incoming reports.

We partner with reputable vendors who are required to comply with specific obligations, including provisions for resiliency, support, transparency, and user privacy.

We are also using machine learning to better detect and action on content and people that should not be using our platform, across all abuse types, including illegal drug sales. We recently shared how we are using machine learning to prevent bad actors like terrorists or scammers from using our platform: https://www.facebook.com/notes/facebook-security/introducing-new-machine-learning-techniques-to-help-stop-scams/10155213964780766/.

4. Why did it take so long to ban the terms within the search function (they have been notified this was a pervasive problem since at least as early as 2011)?

We use a combination of technology and human review to inform Search ranking and we are working to improve our systems to filter from Search instances of illegal drug sales on Facebook.

We have an iterative process to help prevent opportunities for—and respond quickly to—attempts to sell illicit drugs on our platforms. Our Community Standards and other policies make it very clear that buying, selling or trading non-medical or pharmaceutical drugs is not allowed on Facebook. Any time we become aware of content on Facebook that is facilitating activity like illicit drug sales, we remove it and have taken measures to minimize the opportunity for these activities to take place on our platform. We continue to look for ways to get faster at finding and removing this content, working across our policy, operations, product, and partnerships teams.

We also update our detection methods as bad actors work to game the system and bypass our safeguards.

We are committed to finding new and better ways to combat the sale of illegal drugs on Facebook and we will continue to prioritize the issue this year.

5. How many children, teens and other Americans have been harmed in that time due to the failure to act?

The epidemic of addiction is an issue that affects so many families, and no company or government organization can address it alone. We have an iterative process in place to ensure that we prevent opportunities for—and respond quickly to—illicit drug sales on our platforms. We are also working closely with experts to take all possible actions and have explicit policies in place that help make our platform safe for our community.

We are committed to finding new and better ways to combat the sale of illegal drugs on Facebook and we will continue to prioritize the issue this year.

6. Which, if any, experts were consulted to help identify which controlled substances to identify and ban from the search function?

We consulted publicly available resources from a number of federal agencies, including the Food and Drug Administration and the National Institute on Drug Abuse. We also consulted our internal safety experts as well as our NGO partners, including Partnership for Drug Free Kids.

7. While the search terms have been banned, the content that facilitates the illegal sale of drugs continues unaffected, this is illegal counterfeit medicines continue to be sold unabated in newsfeeds, posts, event pages, groups, etc.

We remove content on Facebook that is facilitating the sale of illegal drugs once we are made aware of it. We make it easy for people to report any piece of content on Facebook—profiles, Pages, Groups, individual content and even comments. We encourage our community to continue to tell us if they see this behavior anywhere on our service.

In addition to responding to reports from our community about this content on Facebook, we also have a process to identify and remove content. We are very focused on continuing to look for ways to get faster at finding and removing this content, working across policy, operations, product, and partnerships. And we are constantly updating our detection methods as bad actors work to game the system.

If we identify violating content, we are able to look for associated profiles, Pages, groups, hashtags and accounts and remove them.

We have also made it harder for people to find content that facilitates the sale of opioids on our platform. We are constantly updating this approach as bad actors find new ways to bypass our safeguards.

Something important we have to keep in mind is that bad actors in this space will continue to update their tactics and even the terminology they use, to avoid detection. Even when we're talking about our efforts around opioid sales there is an opportunity for bad actors to learn about our latest efforts, so they can change their activity to avoid detection. We continue in our efforts to stay on the pulse of emerging trends by bad actors conducting this illicit activity and we are constantly updating this approach as bad actors find new ways to bypass our safeguards.

8. How does Facebook plan to "self-regulate" moving forward?

Facebook is generally not opposed to regulation but wants to ensure it is the right regulation. We are already regulated in many ways—for example, under the Federal Trade Commission Act—and we are subject to ongoing oversight by the FTC under the terms of a 2011 Consent Order. Moreover, Facebook has inherent incentives to protect its customers' privacy and address breaches and vulnerabilities. Indeed, the recent discovery of misconduct by an app developer on the Facebook platform clearly hurt Facebook and made it harder for us to achieve our social mission. As such, Facebook is committed to protecting our platform from bad actors, ensuring we are able to continue our mission of giving people a voice and bringing them closer together. We are also actively building new technologies to help prevent abuse on our platform, including advanced AI tools to monitor and remove fake accounts. We have also significantly increased our investment in security, employing more than 15,000 individuals working solely on security and content review and planning to increase that number to over 20,000 by the end of the year. We have also strengthened our advertising policies, seeking to prevent discrimination while improving transparency.

The Honorable Adam Kinzinger

1. I am a combat veteran and I continue to serve in the Air Guard. The collective security of my constituents—and all Americans—factors into many of the decisions I make on their behalf in Congress. In national security matters, I analyze and address the current threat environment with the best available data, intelligence, and strategic thinking. But it is not enough to analyze the current threat environment and simply react. We must anticipate future threat environments and strategize accordingly. Facebook's new bug bounty program is a good step to address both current and future threats. But broadly speaking:

a. What threats do you anticipate in the future? And—other than bug bounties and additional security personnel—what is Facebook doing today to mitigate the threats of tomorrow?

We are working hard to regain the trust of our community.

Success would consist of minimizing or eliminating abuse of our platform and keeping our community safe. We have a number of specific goals that we will use to measure our progress in these efforts. First, we are increasing the number of people working on safety and security at Facebook, to 20,000. We have significantly expanded the number of people who work specifically on election integrity, including people who investigate this specific kind of abuse by foreign actors. Those specialists find and remove more of these actors. Second, we work to improve threat intelligence sharing across our industry, including, we hope, by having other companies join us in formalizing these efforts. This is a fight against sophisticated actors, and our entire industry needs to work together to respond quickly and effectively. Third, we are bringing greater transparency to election ads on Facebook by requiring more disclosure from people who want to run election ads about who is paying for the ads and by making it possible to see all of the ads that an advertiser is running, regardless of the targeting. We believe that these efforts will help to educate our community and to arm users, media, civil society, and the government with information that will make it easier to identify more sophisticated abuse to us and to law enforcement.

We have gotten increasingly better at finding and disabling fake accounts. We're now at the point that we block millions of fake accounts each day at the point of creation before they do any harm.

We are taking steps to help users assess the content they see on Facebook. For example, for ads with political content, we've created an archive that will hold ads with political content for seven years—including for information about ad impressions and spend, as well as demographic data such as age, gender and location. People in Canada and Ireland can already see all the ads that a Page is running on Facebook—and we've launched this globally. Further, advertisers will now need to confirm their ID and location before being able to run any ads with political content in the US. All ads with political content will also clearly state who paid for them. We also want to empower people to decide for themselves what to read, trust, and share. We promote news literacy and work to inform people with more context. For example, if third-party fact-checkers write articles about a news story, we show them immediately below the story

in the Related Articles unit. We also notify people and Page Admins if they try to share a story, or have shared one in the past, that's been determined to be false.

2. It is no secret that Facebook is used to influence voters. Given recent concerns with Russia's attempts to subvert our democratic process—and knowing that other state actors will likely attempt similar campaigns:

a. What tools will you use to defend not only your platform, but by extension, our republic and our national security?

In the run-up to the 2016 elections, we were focused on the kinds of cybersecurity attacks typically used by nation states, for example phishing and malware attacks. And we were too slow to spot this type of information operations interference. Since then, we've made important changes to prevent bad actors from using misinformation to undermine the democratic process.

This will never be a solved problem because we're up against determined, creative and well-funded adversaries. But we are making steady progress. Here is a list of the 10 most important changes we have made:

- **Ads transparency.** Advertising should be transparent: users should be able to see all the ads an advertiser is currently running on Facebook, Instagram and Messenger. And for ads with political content, we've created an archive that will hold ads with political content for seven years—including information about ad impressions and spend, as well as demographic data such as age, gender and location. People in Canada and Ireland have already been able to see all the ads that a Page is running on Facebook—and we've launched this globally.

- **Verification and labeling.** Every advertiser will now need to confirm their ID and location before being able to run any ads with political content in the US. All ads with political content will also clearly state who paid for them.

- **Updating targeting.** We want ads on Facebook to be safe and civil. We thoroughly review the targeting criteria advertisers can use to ensure they are consistent with our principles. As a result, we removed nearly one-third of the targeting segments used by the IRA. We continue to allow some criteria that people may find controversial. But we do see businesses marketing things like historical books, documentaries or television shows using them in legitimate ways.

- **Better technology.** Over the past year, we've gotten increasingly better at finding and disabling fake accounts. We now block millions of fake accounts each day as people try to create them—and before they've done any harm. This is thanks to improvements in machine learning and artificial intelligence, which can proactively identify suspicious behavior at a scale that was not possible before—without needing to look at the content itself.

- **Action to tackle fake news.** We are working hard to stop the spread of false news. We work with third-party fact-checking organizations to limit the spread of articles

rated false. To reduce the spread of false news, we remove fake accounts and disrupt economic incentives for traffickers of misinformation. We also use various signals, including feedback from our community, to identify potential false news. In countries where we have partnerships with independent third-party fact-checkers, stories rated as false by those fact-checkers are shown lower in News Feed. If Pages or domains repeatedly create or share misinformation, we significantly reduce their distribution and remove their advertising rights. We also want to empower people to decide for themselves what to read, trust, and share. We promote news literacy and work to inform people with more context. For example, if third-party fact-checkers write articles about a news story, we show them immediately below the story in the Related Articles unit. We also notify people and Page Admins if they try to share a story, or have shared one in the past, that's been determined to be false. In addition to our own efforts, we're learning from academics, scaling our partnerships with third-party fact-checkers and talking to other organizations about how we can work together.

A key focus is working to disrupt the economics of fake news. For example, preventing the creation of fake accounts that spread it, banning sites that engage in this behavior from using our ad products, and demoting articles found to be false by fact checkers in News Feed—causing it to lose 80% of its traffic. We now work with independent fact checkers in the US, France, Germany, Ireland, the Netherlands, Italy, Mexico, Colombia, India, Indonesia and the Philippines with plans to scale to more countries in the coming months.

- **Significant investments in security.** We're doubling the number of people working on safety and security from 10,000 last year to over 20,000 this year. We expect these investments to impact our profitability. But the safety of people using Facebook needs to come before profit.

- **Industry collaboration.** Recently, we joined 34 global tech and security companies in signing a TechAccord pact to help improve security for everyone.

- **Information sharing and reporting channels.** In the 2017 German elections, we worked closely with the authorities there, including the Federal Office for Information Security (BSI). This gave them a dedicated reporting channel for security issues related to the federal elections.

- **Tracking 40+ elections.** In recent months, we've started to deploy new tools and teams to proactively identify threats in the run-up to specific elections. We first tested this effort during the Alabama Senate election, and plan to continue these efforts for elections around the globe, including the US midterms. Last year we used public service announcements to help inform people about fake news in 21 separate countries, including in advance of French, Kenyan and German elections.

- **Action against the Russia-based IRA.** In April, we removed 70 Facebook and 65 Instagram accounts—as well as 138 Facebook Pages—controlled by the IRA primarily targeted either at people living in Russia or Russian-speakers around the world including from neighboring countries like Azerbaijan, Uzbekistan and Ukraine.

The IRA has repeatedly used complex networks of inauthentic accounts to deceive and manipulate people in the US, Europe and Russia—and we don't want them on Facebook anywhere in the world.

3. In these hearings you discussed Facebook's processes to remove inappropriate content. You described the evolution of these processes—past, present, and future. You said Facebook is developing artificial intelligence in the next 5-10 years to do more on this front with less user input. But once something is uploaded, it can be downloaded to a computer or spread over the Internet in seconds. Since the hearing, I have been informed by Facebook employees that the company does block child pornography at the point of upload, which I applaud. But in cases of other types of clearly illegal or highly inappropriate content:

a. Is blocking at the point of upload not the most effective means of preventing the spread of this information or these files? What barriers exist for Facebook in terms of implementing this sort of system?

We work tirelessly to identify and report child exploitation images (CEI) to appropriate authorities. We identify CEI through a combination of automated and manual review. On the automated review side, we use image hashing to identify known CEI. On the manual review side, we provide in-depth training to content reviewers on how to identify possible CEI. Confirmed CEI is reported to the NCMEC, which then forwards this information to appropriate authorities.

We are using machine learning to better detect and action on other content and people that should not be using our platform. We recently shared how we are using machine learning to prevent bad actors like terrorists or scammers from using our platform (https://www.facebook.com/notes/facebook-security/introducing-new-machine-learning-techniques-to-help-stop-scams/10155213964780766/).

Of course, we cannot rely on technology alone to keep our community safe. Known CEI is contraband regardless of how it is shared, so no review is required before we block it on upload. The same is not true in other situations. For example, a photo of an armed man waving an ISIS flag might be propaganda or recruiting material, but could be an image in a news story. To understand context and more nuanced cases, we need human expertise.

4. You and I had an exchange during the hearing on this topic, but I wish to provide additional background for my questions so that you may provide detailed answers in writing using the proper context.

Given the global reach of Facebook, I would like to know more about the company's policies and practices with respect to information sharing with foreign governments. In 2014, the Government of Russia enacted a law (Russian Federal Law No. 242-FZ), which became effective September 1, 2015. The law requires social media companies to have a physical presence in Russia. While you explained during the hearing that Facebook does not have a physical presence in Russia, the Government of Russia (albeit an unreliable source of information) claims that Facebook has

agreed to comply with this law. With this context, I reiterate here some of my same questions, and have included other relevant questions:

a. What personal data does Facebook make available from Facebook, Instagram, and Whatsapp to Russian state agencies, including intelligence and security agencies?

As part of official investigations, government officials sometimes request data about people who use Facebook. We have strict processes in place to handle these government requests, and we disclose account records solely in accordance with our terms of service and applicable law. We require officials to provide a detailed description of the legal and factual basis for their request, and we push back if the request appears to be legally deficient or is overly broad, vague, or otherwise inconsistent with our policies. Further, with respect to government requests for disclosure from outside the United States, a Mutual Legal Assistance Treaty request or letter rogatory may be required to compel the disclosure of the contents of an account.

As part of our ongoing effort to share information about the requests we have received from governments around the world, Facebook regularly produces a Transparency Report about government data requests to Facebook. Our Transparency Report contains historical information about Russian requests for data going back to 2013. In summary, we received 34 requests from the Russian government between 2013 and 2017. We did not provide any data in response to these requests. See https://transparency.facebook.com/government-data-requests/country/RU.

b. Is this data only from accounts located in, or operated from, these individual countries? Or does it include Facebook's data on users across the world?

See Response to Question 4(a).

c. Does Facebook do this with other foreign governments, for instance, China, Iran, or Syria?

i If Facebook shares data with any foreign governments, please provide a comprehensive list of these countries, their respective state agencies, and the specific types of data sets shared.

As part of our ongoing effort to share information about the requests we have received from governments around the world, Facebook regularly produces a Transparency Report about government data requests to Facebook, including any requests from China, Iran, or Syria. See https://transparency.facebook.com/government-data-requests.

d. Did Facebook delete any data related to Russian information operations conducted against the United States?

i If so, please disclose to this Committee all relevant information about any and all data that was, or may have been, deleted.

ii If not, will you agree to make all of this data and content available to our national security, law enforcement, and intelligence agencies?

Will you make it available to Congress? Will you make it available to researchers?

Facebook has taken appropriate steps to retain relevant information related to IRA activity on Facebook.

5. In your testimony at the Senate hearing you stated that "Facebook is responsible for the content on Facebook." I want to discuss cyber bullying and how parents and young adults use Facebook. I do not believe our laws from the 20th century have caught up with social media in the 21st century. Parents, teachers, social networks, as well as federal and state governments, must address how this technology can hurt innocent people. In Illinois, there are laws that prevent people from distributing personal photos with malicious intent. A fake account can be created in a matter of minutes on Facebook to distribute personally damaging photos that will target individuals and tarnish a reputation, perhaps permanently.

a. Given your statement from the Senate hearing, what role does Facebook have in the harm that this creates?

Under our Community Standards, we remove content that appears to purposefully target private individuals with the intention of degrading or shaming them. We also want to prevent unwanted or malicious contact on the platform.

In the case of the most malicious content that can have devastating impact on the victims, child exploitation imagery (CEI) and the non-consensual sharing of intimate imagery (NCII), we use photo-matching technologies to thwart the sharing of known images. In addition, we will disable accounts for sharing CEI and NCII; and we report the sharing of CEI to the National Center for Missing and Exploited Children (NCMEC).

In addition, we use technologies to help us identify and remove fake accounts. We block millions of fake accounts every day when they are created and before they can do any harm. Between January and March of 2018, for example, 583 million fake accounts were disabled, usually within minutes of registration.

b. How can Facebook increase the effectiveness and timeliness of its responses to users' claims that they are victims of cyber bullying and fake accounts?

Facebook encourages users to report to us bullying and harassment, as well as other content that may violate our policies. Our Community Operations team works hard to review those reports and takes action when content violates our policies. Even if user-reported content does not violate our policies, however, users have control over what they see and who they interact with. A user can:

- Block someone, which prevents the other person from seeing things the user posts on his/her profile; starting conversations with the user; adding the user as a friend; tagging the user in posts, comments, or photos; and inviting the user to events or groups.

- Unfriend someone, which prevents the other person from posting on the user's timeline.

- Block someone's messages, which means they will no longer be able to contact the user in Messenger or in Facebook chat. A user can also ignore a Messenger conversation, which automatically moves it out of the user's inbox.

- Unfollow someone, which means the person's post will not appear in News Feed. On Instagram, a user can prevent someone from commenting on the user's photos and videos and can also block someone from finding the user's profile, posts or story.

In addition, we have partnered with the Yale Center for Emotional Intelligence to create the Bullying Prevention Hub, available at https://www.facebook.com/safety/bullying. This is a resource for teens, parents and educators seeking support and help for issues related to bullying and other conflicts. It offers step-by-step plans, including guidance on how to start some important conversations for people being bullied, parents who have had a child being bullied or accused of bullying, and educators who have had students involved with bullying.

Our efforts to combat bullying online and offline, including our policies, tools for blocking, reporting and social resolution, programming, and resources, such as our Bullying Prevention Hub and Safety Center, have been effective in combating bullying on Facebook and have helped combat the culture of bullying offline that almost always is connected to online bullying. As noted above, bullying violates our policies and we review reports of content that may constitute bullying or harassment and remove violating content from our platform.

We are building new tools so that we can more quickly and effectively detect abusive, hateful, or false content. We have, for example, designated several hate figures and organizations for repeatedly violating our hate speech policies, which has led to the removal of accounts and content that support, praise, or represent these individuals or organizations. We are also investing in artificial intelligence that will help us improve our understanding of dangerous content.

6. Much of the two hearings focused on third-party apps that use Facebook as a platform to harvest data. But I would like to know about other ways in which third parties might be able to harvest user data.

a. When a user is scrolling through their newsfeed, sees a news article, and clicks it to read it within the Facebook app, is a user's personal information or any other data made available to the media outlet who published the article?

b. When I "Like" or "Follow" a page—such as a news source or a political candidate—are those entities collecting (or able to collect) users' personal information or other user data in any way?

Facebook does not sell people's information to anyone, and we never will. We also impose strict restrictions on how our partners can use and disclose the data we provide. Our data privacy policy makes clear the circumstances in which we work with third-party partners who

help us provide and improve our Products or who use Facebook Business Tools to grow their businesses, which makes it possible to operate our companies and provide free services to people around the world.

We do not share any personal information with media outlets based on people's viewing or clicking on the media outlet's content on News Feed. Of course, if a person clicks on a link and goes to the media outlet's website where the person previously logged in using any system, including Facebook Login, then the media outlet could know who was viewing the content on its website.

People have control over the audience of their "likes" and "follows." If the "like" or "follow" is public, then the Page will be able to see who liked them (including their public profile info). If it is not public, then the Page will not get personal information about the person, but will have access to aggregate analytics about all the people engaging with the page.

7. The terms of service for Instagram indicate that the company monitors users' scrolling movements,

a. Will you describe in as much detail as possible the reasons for this type of monitoring and specific methods employed?

The reference you describe comes from our newly updated Data Policy, which describes how we use data across our products, including Instagram and Facebook. Facebook receives and uses information about scrolling movements to improve its products and experiences. For example, when a user scrolls downward, we use that information to load more posts in a users' feed, and information about scrolling can help us improve the design of our products. In addition, scrolling movements can help us detect and prevent harm and fraud by distinguishing humans from bots.

8. Facebook has changed its privacy policies and privacy settings a number of times over the years.

a. How many times has Facebook executed a proactive, high-profile campaign to inform users of these changes and tell them that they are "now empowered" to control their information and privacy?

b. Given what users now know, how many of those times would you say that has proven to be true?

Our approach to control is based on the belief that people should be able to choose who can see what they share and how their data shapes their experience on Facebook and should have control over all data collection and uses that are not necessary to provide and secure our service. We recognize, however, that controls are only useful if people know how to find and use them. That is why we continuously deliver in-product educational videos in people's News Feeds on important privacy topics like how to review and delete old posts and what it means to delete an account. We are also inviting people to take our Privacy Checkup—which prompts people to review key data controls—and we are sharing privacy tips in education campaigns off of

Facebook, including through ads on other websites. To make our privacy controls easier to find, we are launching a new settings menu that features core privacy settings in a single place.

We are constantly improving and iterating on these controls and education to provide a better experience for people. We regularly provide people with notice through various channels about changes to our product, including improvements on privacy controls. We are always working to improve our controls and do not view this as something that is ever likely to be finished.

9. After the widespread coverage of the Cambridge Analytica incident, Facebook announced some corrective actions and new practices on March 21, 2018. The company said it would investigate apps that had access to "large amounts of [user] information" prior to the 2014 policy changes. The announcement also stated there would be audits of apps that display "suspicious activity". I also understand that the company will now require third-party app developers to sign a contract before asking users for access to posts or other private data.

a. What does Facebook consider a "large amount of information" in this context—is there a numeric threshold? If so, what is that threshold?

b. Further, what does Facebook consider to be "suspicious activity"? Please provide at least three examples.

In general, an app will be reviewed if (among other reasons, e.g., escalation through Data Bounty) it launched prior to the changes we made to platform policies in 2014, if it had a significant number of users and if the app sought to access significant or unexpected data fields. Our investigation is ongoing and as part of it we are taking a close look at applications that had access to friends data under Graph API V1 before we made technical changes to our platform to change this access.

10. Regarding the practice of requiring third party developers to sign contracts, I do not understand how or why this was never a practice before the Cambridge Analytica incident. Let us suppose a purely hypothetical scenario in which Facebook rids itself of its mission statement of "connecting people" and only cares about monetizing data.

a. Is it not good sense from a legal and business perspective to require some strong legal agreements with these developers so that Facebook could take legal action against an entity that blatantly violates the agreed-upon terms?

b. Why did Facebook not believe this was necessary before the Cambridge Analytica incident?

We use a variety of tools to enforce Facebook policies against violating parties, including developers. We review tens of thousands of apps per year and regularly disapprove noncompliant apps as part of our proactive review process. We also use tools like cease-and-desist letters, account suspensions, letter agreements, and civil litigation. For example, since 2006, Facebook

has sent over 1,150 cease-and-desist letters to over 1,600 targets. In 2017, we took action against about 370,000 apps, ranging from imposing certain restrictions to removal of the app from the platform. Moreover, we have required parties who have procured our data without authorization to delete that data. We have invested significant resources in these efforts. Facebook is presently investigating apps that had access to large amounts of information before we changed our platform policies in 2014 to significantly reduce the data apps could access. As of early June 2018, around 200 apps (from a handful of developers: Kogan, AIQ, Cube You, the Cambridge Psychometrics Center, myPersonality, and AIQ) have been suspended—pending a thorough investigation into whether they did in fact misuse any data.

Additionally, we have suspended an additional 14 apps, which were installed by around one thousand people. They were all created after 2014, after we made changes to more tightly restrict our platform APIs to prevent abuse. However, these apps appear to be linked to AIQ, which was affiliated with Cambridge Analytica. So, we have suspended them while we investigate further. Any app that refuses to take part in or fails our audit will be banned.

11. A news report in March 2018 indicated that former Obama for America campaign officials worked with your company in the lead-up to the 2012 elections to allow users to sign into the campaign website through Facebook, and they used that connection to harvest data not only about those people who signed in, but their "Friends" as well. And by Facebook's own statements, we know that your company knew about the Cambridge Analytica data harvesting incident sometime in 2015. Further, your testimony indicates that you detected Russian threats in 2016 ahead of the elections. I have received no indication that Facebook disclosed these incidents to their users or the general public until sometime last month, despite the first of these incidents taking place about 6 years ago.

a. In terms of disclosure of these incidents to the federal government:

i Which of these three incidents, if any, did Facebook disclose to the federal government?

ii How long after discovery did it take Facebook to disclose the incident(s) to the federal government? Please provide dates relating to the discovery of these incidents as well as their disclosure to the federal government.

b. In terms of disclosure of these instances to Facebook users and the general public:

i Why wasn't Facebook forthright with its users about these incidents? In your response, please disclose, in as much detail as possible, any other undisclosed incidents of data harvesting.

Prior to May 2014, Facebook's developer Graph API allowed app developers to request consent to access information from the installing user—such as name, gender, birthdate, location (i.e., current city or hometown), photos and Page likes—and also (depending on, and in

accordance with, each friend's own privacy settings) the same or similar categories of information that the user's friends had shared with the installing user. Permitting users to reshare friends data available to them on Facebook had the upside of allowing people to take their Facebook data off Facebook to receive a range of new and social experiences off Facebook, beyond those Facebook itself offered. For example, a Facebook user might want to use a music app that allowed the user to (1) see what his or her friends were listening to and (2) give the app permission to access the user's friend list and thereby know which of the user's friends were also using the app. Such access to information about an app user's friends required not only the consent of the app user, but also required that the friends whose data would be accessed have their own privacy settings set to permit such access by third-party apps. Kogan's app received friends' data shared with the installing user (provided the friend's privacy setting permitted such sharing) as any other developer would have at the time. However, he breached our developer terms by transferring the data users consented to share with his app to Cambridge Analytica.

When Facebook learned about Kogan's breach of Facebook's platform policies in December 2015, it took immediate action. The company retained an outside firm to assist in investigating Kogan's actions, to demand that Kogan and each party he had shared data with delete the data and any derivatives of the data, and to obtain certifications that they had done so. Because Kogan's app could no longer collect most categories of data due to changes in Facebook's platform, the company's highest priority at that time was ensuring deletion of the data that Kogan may have accessed before these changes took place. With the benefit of hindsight, we wish we had notified people whose information may have been impacted. Facebook has since notified all people potentially impacted with a detailed notice at the top of their News Feed.

Unlike Kogan and his company, GSR, Facebook is not aware that any Facebook app operated by the 2012 Obama for America campaign violated our Platform Policies. Further, during the 2012 election cycle, both the Obama and Romney campaigns had access to the same tools, which are the same tools that every campaign is offered.

With respect to Russia, we learned from press accounts and statements by congressional leaders that Russian actors might have tried to interfere in the 2016 election by exploiting Facebook's ad tools. This is not something we had seen before, and so we started an investigation. We found that fake accounts associated with the IRA spent approximately $100,000 on around 3,500 Facebook and Instagram ads between June 2015 and August 2017. Our analysis also showed that these accounts used these ads to promote the roughly 120 Facebook Pages they had set up, which in turn posted more than 80,000 pieces of content between January 2015 and August 2017. The Facebook accounts that appeared tied to the IRA violated our policies because they came from a set of coordinated, inauthentic accounts. We shut these accounts down and began trying to understand how they misused our platform. We shared the ads we discovered with Congress, in a manner that is consistent with our obligations to protect user information, to help government authorities complete the vitally important work of assessing what happened in the 2016 election. The ads (along with the targeting information) are publicly available at https://democrats-intelligence.house.gov/facebook-ads/social-media-advertisements.htm.

12. With respect to third-party applications that are linked with Facebook, reports indicate that there are more than 9 million of these third-party apps. These numbers indicate to me just how valuable consumer data is to Facebook and a litany of other entities.

a. I understand Facebook does not design these apps, but from your perspective, is it safe to say that a large portion of them are designed primarily around the harvesting of your users' data rather than making social connections or providing some sort of interactive entertainment?

Facebook's policies regarding third-party usage of its platform technologies have prohibited—and continue to prohibit—third-party app developers from selling or licensing user data obtained from Facebook and from sharing any user data obtained from Facebook with any ad network, data broker or other advertising or monetization-related service. We will investigate all apps that had access to large amounts of information before we changed our platform in 2014 to reduce data access, and we will conduct a full audit of any app with suspicious activity.

b. If you agree, should Facebook reconsider its relationships with these third-party app developers? If so, how? If not, why not?

In early 2014, Facebook introduced changes to provide users more choice and control over what information apps received, to reduce the amount of data that could be shared with third-party apps, and to establish a new review and approval process for any new apps that sought to request anything more than basic information about the installing user. These changes reflected the tradeoffs between data portability and app innovation, on the one hand, and privacy and control, on the other, that we felt were right for people based on user feedback and the experiences enabled by our platform at that time. These changes accompanied a new version of the platform API, called Graph API V2, which incorporated several key new elements.

Recently, we announced a number of additional steps we're taking to address concerns raised by Kogan's app.

- **Review our platform.** We will investigate all apps that had access to large amounts of data before the platform changes we announced in 2014, and we will audit any app where we identify suspicious activity. If we identify misuses of data, we'll take immediate action, including banning the app from our platform and pursuing legal action if appropriate.

- **Tell people about data misuse.** We will tell people about apps that have misused their data.

- **Turn off access for unused apps.** If someone has not used an app within the last three months, we will turn off the app's access to their data.

- **Restrict Facebook Login data.** We are changing Login, so that the only data that an app can request without app review will include name, profile photo, and email address. Requesting any other data will require approval from Facebook. We will also

no longer allow apps to ask for access to information like religious or political views, relationship status and details, custom friends lists, education and work history, fitness activity, book reading and music listening activity, news reading, video watch activity, and games activity. We will encourage people to manage the apps they use. We already show people what apps their accounts are connected to and allow them to control what data they've permitted those apps to use. But we're making it easier for people to see what apps they use and the information they have shared with those apps.

- **Reward people who find vulnerabilities.** We launched the Data Abuse Bounty program so that people can report to us any misuses of data by app developers.

- **Update our policies.** We have updated our terms and Data Policy to explain how we use data and how data is shared with app developers.

13. Facebook earned about $40 billion in revenue last year, most of which is derived from advertising sales. You have the resources to identify and mitigate the threats of bots, the distribution of child pornography, and the effects of posting ISIS videos on the unsuspecting public. I would not be the first to say that I think Facebook could do better at each of those things, but in fairness, I appreciate the fact that you are hiring thousands of more people to assist on these fronts. But with respect to smaller startup tech companies who do not have the resources to confront these issues:

a. What are their barriers to market entry for these startups?

b. Are the barriers financial, regulatory, or something else?

In Silicon Valley and around the world, new social apps are emerging all the time. The average American uses eight different apps to communicate with their friends and stay in touch with people. There is a lot of choice, innovation, and activity in this space, with new competitors arising all the time. Facebook's top priority and core service is to build useful and engaging products that enable people to connect, discover and share through mobile devices and personal computers. Given its broad product offerings, Facebook faces numerous competitors, competing to attract, engage, and retain users, to attract and retain marketers, and to attract and retain developers who build compelling mobile and web applications. For instance, if a user wants to share a photo or video, they can choose between Facebook, DailyMotion, Snapchat, YouTube, Flickr, Twitter, Vimeo, Google Photos, and Pinterest, among many other services. Similarly, if a user is looking to message someone, just to name a few, there's Apple's iMessage, Telegram, Skype, Line, Viber, WeChat, Snapchat, and LinkedIn—as well as the traditional text messaging services their mobile phone carrier provides. Equally, companies also have more options than ever when it comes to advertising—from billboards, print and broadcast, to newer platforms like Facebook, Spotify, Twitter, Google, YouTube, Amazon or Snapchat. Facebook represents a small part (in fact, just 6%) of this $650 billion global advertising ecosystem and much of that has been achieved by helping small businesses—many of whom could never have previously afforded newspaper or TV ads—to cost-effectively reach a wider audience.

More generally, in Silicon Valley and around the world, new social apps are emerging all the time. The average American uses eight different apps to communicate with their friends and stay in touch with people. There is a lot of choice, innovation, and activity in this space, with new competitors arising all the time. Facebook's top priority and core service is to build useful and engaging products that enable people to connect, discover and share through mobile devices and personal computers.

With respect to any regulatory barriers, as the internet becomes more important in people's lives, a critical question is the right set of regulations that should apply to all internet services, regardless of size.

14. In 2011, the Federal Trade Commission charged, among other things, that Facebook had failed to disclose to users that their choices to restrict profile information to "Only Friends" or "Friends of Friends" would not work with respect to certain third parties, including apps; and after making changes to its privacy policy, failed to adequately disclose that one of its recent privacy changes overrode existing user privacy settings.

Even if a user kept track of their privacy settings and wished to restrict access, their choices were overridden by this top-down overhaul of privacy policies—all with little or no warning

a. Would you say that providing users the option to limit their information to only "Friends Only" or "Friends of Friends" was disingenuous?

b. Who at Facebook made that decision? Why was that decision made?

We furnished extensive information to the FTC regarding the ability for users to port their Facebook data (including friends data that had been shared with them) with apps on Facebook's platform, as part of the FTC's investigation culminating in the July 27, 2012 Consent Order. The Consent Order memorializes the agreement between Facebook and did not require Facebook to turn off the ability for people to port friends data that had been shared with them on Facebook to apps they used. Facebook voluntarily changed this feature of the Platform in 2014, however.

In 2011, Facebook offered more control and protection over the availability of friends data to apps than any other digital platform at the time, including mobile app platforms, which generally permitted apps to access user data and their friends' data without consent or any control. By contrast, Facebook notified users of each category of data an app could access—including friends data—before the user consented to the app, and also provided all users with controls that would prevent their friends from sharing their data with apps on Facebook's platform.

15. In 2010, Facebook engaged in a campaign to inform users that they were requiring applications to obtain specific approval before gaining access to any personal information that a user has not made publicly available under the "Everyone" setting.

a. At that time, what mechanisms or procedures were also put in place to verify—or even spot-check—that third-party apps were actually obtaining explicit approval from users before accessing their information? Please provide specifics.

In 2007, there was industry-wide interest in enriching and expanding users' experiences on various platforms by allowing them to take their data (from a device or service) to third-party developers to receive new experiences. For example, around that time, Apple and Google respectively launched their iOS and Android platforms, which were quickly followed by platform technologies and APIs that allowed developers to develop applications for those two platforms and distribute them to users through a variety of channels. Similarly, in 2007, Facebook launched a set of platform technologies that allowed third parties to build applications that could run on and integrate with the Facebook service and that could be installed by Facebook users who chose to do so. In December 2009, Facebook launched new privacy controls that enabled users to control which of the types of information that they made available to their friends could be accessed by apps used by those friends.

As with all of these platforms, the permissions model that governed the information that third-party applications could access from the Platform evolved. For example, in April 2010, Facebook launched granular data permissions (GDP), which allowed users to examine a list of categories of information that an app sought permission to access before they authorized the app.

Throughout the relevant period and through today, Facebook's policies regarding third-party usage of its platform technologies have prohibited—and continue to prohibit—third-party app developers from selling or licensing user data obtained from Facebook or from sharing any user data obtained from Facebook with any ad network, data broker or other advertising or monetization-related service.

In November 2013, when Kogan launched the app, apps generally could be launched on the Platform without affirmative review or approval by Facebook. The app used the Facebook Login service, which allowed users to utilize their Facebook credentials to authenticate themselves to third-party services. Facebook Login and Facebook's Graph API also allowed the app to request permission from its users to bring their Facebook data (their own data and data shared with them by their friends) to the app, to obtain new experiences.

At that time, the Graph API V1 allowed app developers to request consent to access information from the installing user such as name, gender, birthdate, location (i.e., current city or hometown), photos and Page likes—and also (depending on, and in accordance with, each friend's own privacy settings) the same or similar categories of information the user's friends had shared with the installing user. Permitting users to share data made available to them by their friends had the upside of making the experience of app users more personalized and social. For example, a Facebook user might want to use a music app that allowed the user to (1) see what his or her friends were listening to and (2) give the app permission to access the user's friend list and thereby know which of the user's friends were also using the app. Such access to information about an app user's friends required not only the consent of the app user, but also required that the friends whose data would be accessed have their own privacy settings set to permit such

access by third-party apps. In other words, Kogan's app could have accessed a user's friends' information only for friends whose privacy settings permitted such sharing.

In April 2014, we announced that we would more tightly restrict our platform APIs to prevent abuse. At that time, we made clear that existing apps would have a year to transition—at which point they would be forced (1) to migrate to the more restricted API and (2) be subject to Facebook's new review and approval protocols. The vast majority of companies were required to make the changes by May 2015; a small number of companies (fewer than 100) were given a one-time extension of less than six months beyond May 2015 to come into compliance. (One company received an extension to January 2016.) In addition, in the context of our ongoing review of third-party apps, we discovered a very small number of companies (fewer than 10) that theoretically could have accessed limited friends' data as a result of API access that they received in the context of a beta test. We are not aware that any of this handful of companies used this access, and we have now revoked any technical capability they may have had to access any friends' data.

New apps that launched after April 30, 2014 were required to use our more restrictive platform APIs, which incorporated several key new elements, including:

- Institution of a review and approval process, called App Review (also called Login Review), for any app seeking to operate on the new platform that would request access to data beyond the user's own public profile, email address, and a list of friends of the user who had installed and authorized the same app;

- Generally preventing new apps on the new platform from accessing friends data without review; and

- Providing users with even more granular controls over their permissions as to what categories of their data an app operating on the new platform could access.

Our investigation is ongoing and as part of it we are taking a close look at applications that had access to friends data under Graph API V1 before we made technical changes to our platform to change this access.

The App Review process introduced in 2014 required developers who create an app that asks for more than certain basic user information to justify the data they are looking to collect and how they are going to use it. Facebook then reviewed whether the developer has a legitimate need for the data in light of how the app functions. Only if approved following such review can the app ask for a user's permission to get their data. Facebook has rejected more than half of the apps submitted for App Review between April 2014 and April 2018, including Kogan's second app. We are changing Login so that the only data that an app can request without app review will include name, profile photo, and email address.

The Honorable Gus Bilirakis

1. What is the point of building new artificial intelligence tools and adding thousands of new security and content reviewers if there is no set standard for content review or consistency of outcome, as in the case of my constituent?

Being a platform for all ideas is a foundational principle of Facebook. We are committed to ensuring there is no bias in the work we do. Suppressing content on the basis of political viewpoint or preventing people from seeing what matters most to them is directly contrary to Facebook's mission and our business objectives.

Decisions about whether to remove content are based on whether the content violates our Community Standards. Our Community Standards are global and all reviewers use the same guidelines when making decisions. They undergo extensive training when they join and, thereafter, are regularly trained and tested with specific examples on how to uphold the Community Standards and take the correct action on a piece of content. This training includes when policies are clarified, or as they evolve.

We seek to write actionable policies that clearly distinguish between violating and non-violating content and we seek to make the decision-making process for reviewers as objective as possible.

Our reviewers are not working in an empty room. There are quality control mechanisms as well as management on site to help or seek guidance from if needed. When a reviewer isn't clear on the action to take based on the Community Standards, they can pass the content decision to another team for review. We also audit the accuracy of reviewer decisions on an ongoing basis to coach them and follow up on improving, where errors are being made.

When we're made aware of incorrect content removals, we review them with our Community Operations team so as to prevent similar mistakes in the future.

We recently introduced the right to appeal our decisions on individual posts so users can ask for a second opinion when they think we've made a mistake. As a first step, we are launching appeals for posts that were removed for nudity / sexual activity, hate speech or graphic violence. We are working to extend this process further, by supporting more violation types, giving people the opportunity to provide more context that could help us make the right decision, and making appeals available not just for content that was taken down, but also for content that was reported and left up. We believe giving people a voice in the process is another essential component of building a fair system.

2. One of the main purposes of a Terms of Service agreement is to inform the consenting parties of their rights and obligations in the use of the service. Facebook's Terms of Service, specifically its Data Policy, defines the methods and limitations of information sharing. However, when that portion of the agreement was violated by Global Science Research, users were not notified of the breach of their rights under the Terms of Service.

a. What is the point of having a terms of service agreement if the consumer is not notified upon a breach of such terms?

b. Should an updated Terms of Service agreement include proactive user notification responsibilities on Facebook, similar to its obligation to inform users of changes to the Terms?

c. Will you commit to updating your Terms of Service to proactively inform users within 3 days after you learn of a privacy violation?

We are in the process of investigating every app that had access to a large amount of information before we changed our Platform in 2014. The investigation process is in full swing, and it has two phases. First, a comprehensive review to identify every app that had access to this amount of Facebook data and to focus on apps that present reason for deeper investigation. And second, where we have concerns, we will conduct interviews, make requests for information (RFI)—which ask a series of detailed questions about the app and the data it has access to—and perform audits using expert firms that may include on-site inspections. We have large teams of internal and external experts working hard to investigate these apps as quickly as possible. As of early June 2018, thousands of apps have been investigated and around 200 apps have been suspended—pending a thorough investigation into whether they did in fact misuse any data. Where we find evidence that these or other apps did misuse data, we will ban them and let people know.

These apps relate to a handful of developers: Kogan, AIQ, Cube You, the Cambridge Psychometrics Center, and myPersonality, with many of the suspended apps being affiliated with the same entity. Many of these suspensions include apps that appear to be "test" apps that were never released to the public, and therefore would not have acquired significant user data, although our investigation into these apps is ongoing.

Additionally, we have suspended an additional 14 apps, which were installed by around one thousand people. They were all created after 2014, after we made changes to more tightly restrict our platform APIs to prevent abuse. However, these apps appear to be linked to AIQ, which was affiliated with Cambridge Analytica. So, we have suspended them while we investigate further. Any app that refuses to take part in or fails our audit will be banned.

Facebook monitors its systems for potential breaches of personal data and logs any potential breach in a system that automatically triggers expedited review. Facebook reviews such potential incidents to determine: (i) whether there was in fact an incident; (ii) its root cause, including short- and long-term remediation (if applicable); and (iii) our legal and ethical obligations. Facebook moves quickly to review potential incidents. Because of the fluid nature of an incident, there are no set timelines for completion of reviews and addressing a discovered vulnerability, but any potential breach is escalated for high priority processing.

Facebook notifies users in accordance with its obligations under applicable law and has also notified people in cases where there was no legal obligation to do so but we nevertheless determined it was the right thing to do under the circumstances.

3. The Facebook Data Policy states, and I quote, "We collect information when you visit or use third-party websites and apps that use our services (like when they offer our Like button or Facebook Log-In or use our measurement and advertising services)."

Does this imply that Facebook has a nexus to collect information about its users from every single website that includes the Facebook Like button, regardless of whether a user interacts with it?

Websites and apps choose whether they use Facebook services to make their content and ads more engaging and relevant and whether they share browser data or other information with Facebook or other companies when people visit their sites. These services include:

- Social plugins, such as our Like and Share buttons, which make other sites more social and help people share content on Facebook;
- Facebook Login, which lets people use their Facebook account to log into another website or app;
- Facebook Analytics, which helps websites and apps better understand how people use their services; and
- Facebook ads and measurement tools, which enable websites and apps to show ads from Facebook advertisers, to run their own ads on Facebook or elsewhere, and to understand the effectiveness of their ads.

Many companies offer these types of services and, like Facebook, they also get information from the apps and sites that use them. Twitter, Pinterest, and LinkedIn all have similar Like and Share buttons to help people share things on their services. Google has a popular analytics service. And Amazon, Google, and Twitter all offer login features. These companies—and many others—also offer advertising services. In fact, most websites and apps send the same information to multiple companies each time users visit them.

For example, when a user visits a website, their browser (for example Chrome, Safari or Firefox) sends a request to the site's server. The browser shares a user's IP address, so the website knows where on the internet to send the site content. The website also gets information about the browser and operating system (for example Android or Windows) they're using because not all browsers and devices support the same features. It also gets cookies, which are identifiers that websites use to know if a user has visited before.

A website typically sends two things back to a user's browser: first, content from that site; and second, instructions for the browser to send the user's request to the other companies providing content or services on the site. So, when a website uses one of our services, our users' browsers send the same kinds of information to Facebook as the website receives. We also get information about which website or app our users are using, which is necessary to know when to provide our tools.

In addition, we also enable ad targeting options—called "interests" and "behaviors"—that are based on people's activities on Facebook, and when, where, and how they connect to the internet (such as the kind of device they use and their mobile carrier). These options do not reflect people's personal characteristics, but we still take precautions to limit the potential for advertisers to misuse them.

We do not use web browsing data to show ads to non-users or otherwise store profiles about non-users. Our goal is to show people content (including advertising) that is relevant to their interests. We use information people have provided on Facebook—such as things they've liked or posts they've engaged with—to help determine what people will be interested in. Like most online advertising companies, we also inform our judgments about what ads to show based on apps and websites that people use off of Facebook. People can turn off our use of web browser data and other data from third-party partners to show them ads through a control in Ads Preferences. They can also customize their advertising experience by removing interests that they do not want to inform the Facebook ads they see. In addition, a person's browser or device may offer settings that allow users to choose whether browser cookies are set and to delete them.

The Honorable Bill Flores

1. **With respect to privacy standards, it is important to first consider what the baseline is/should be. When discussing the "virtual person" that each technology platform user establishes online—such as their name, address, personally identifiable information, posts, searches, pictures, geo-location data, online purchases, websites visited, etc., the baseline standard should be that the individual owns the "virtual person" that they have set up online. During the hearing, Mr. Zuckerberg seemed to echo this sentiment and commented that each user owns their virtual presence.**

   With that in mind, does Facebook believe that the U.S. should be taking a lead role in establishing 21st century privacy standards?

We work hard to provide clear information to people about how their information is used and how they can control it. We agree that companies should provide clear and plain information about their use of data and strive to do this in our Data Policy, in in-product notices and education, and throughout our product—and we continuously work on improving this. We provide the same information about our data practices to users around the world and are required under many existing laws—including US laws (e.g., Section 5 of the FTC Act)—to describe our data practices in language that is fair and accurate.

Facebook is generally not opposed to regulation but wants to ensure it is the right regulation. The issues facing the industry are complex, multi-faceted, and affect an important part of peoples' lives. As such, Facebook is absolutely committed to working with regulators, like Congress, to craft the right regulations. Facebook would be happy to review any proposed legislation and provide comments.

2. **Many public agencies and private industries that handle large quantities of personal data—such as financial institutions, health care providers, human resources, etc.—are subject to rules and regulations of the use of that data. In considering Congressional action to enact privacy standards for technology providers along those same lines, the suggested proposal should be as follows:**

   This policy should state that the data of technology users should be held private unless they specifically consent to the use of that data by others.

   This release should be based upon absolute transparency as to what data will be used, how it will be processed, where it will be stored, what algorithms will be applied to it, who will have access it to it, if it will be sold, and to whom it might be sold.

   The disclosure of this information and the associated "opt-in" disclosure should be written in plain, easily understood language; and the associated user actions to opt-in or opt-out should be easy to understand and easy for non-technical users to execute.

The days of the long, scrolling, "fine-print" disclosures with a single check-mark at the bottom should end. In this regard, based upon personal use of Facebook, the company has come a long way in moving toward that objective.

That said, we must move further.

If Congress were to consider such a federal policy change, as detailed above, for the technology industry regarding the practice of privacy standards, can you please describe how this might impact Facebook's business model?

We believe strongly in providing meaningful privacy protections to people. This is why we work hard to communicate with people about privacy and build controls that make it easier for people to control their information on Facebook. For example, Facebook has redesigned its settings menu to make things easier to find and introduced new Privacy Shortcuts. These shortcuts allow users to make their account more secure, control their personal information, control which ads they see, and control who sees their posts and profile information. Facebook has also introduced additional tools to find, download, and delete user data.

We've worked with regulators, legislators, and privacy experts, at both the state and national levels to educate people and businesses about privacy. We believe an important component of any privacy regulation is clear and consistent oversight and enforcement. We intend to continue this collaborative work to promote privacy protections for our community.

Facebook is generally not opposed to regulation but wants to ensure it is the right regulation. The issues facing the industry are complex, multi-faceted, and affect an important part of peoples' lives. As such, Facebook is absolutely committed to working with regulators, like Congress, to craft the right regulations. Facebook would be happy to review any proposed legislation and provide comments.

The Honorable Richard Hudson

1. **Facebook as you have said is a "platform for all ideas." I know you have heard from others about their concerns regarding Facebook's censorship of content, particularly content that may promote Christian beliefs or conservative political beliefs. You addressed some of these concerns already. Additionally, this type of censorship seems to be applied to businesses that sell firearms. As recently as 2017, firearms-related businesses were being singled out by Facebook and denied the ability to conduct constitutionally-protected commerce – even for items unrelated to firearms. The reason provided for these actions was simply that they linked to their website where they sold firearms, despite the fact that the link was not included in the ad. The case I am familiar with was attempting to advertise American flags.**

    a. **I understand your policies prohibit advertising the sale of weapons, but how can you justify limiting this form of free speech simply because it originates from a business that also sells firearms? How have you updated your policies to ensure users are notified of these standards and you are applying them equally?**

    b. **Could you please explain the measures Facebook takes to ensure constitutionally- protected commercial free speech, as it was recognized by the 9th Circuit Court's three-judge panel ruling in Teixeira vs. Alameda County, which reads "the right to purchase and sell firearms is part and parcel of the historically recognized right to keep and bear arms."?**

Similar to our Community Standards, we have Advertising Policies that outline which ads are and are not allowed on Facebook. Unlike posts from friends or Pages, ads receive paid distribution. This means we have an even higher standard for what is allowed.

During the ad review process, we'll check an ad's images, text, targeting, and positioning, in addition to the content on an ad's landing page. An ad may not be approved if the landing page content isn't fully functional, doesn't match the product/service promoted in the ad, or doesn't fully comply with our Advertising Policies.

Per our Advertising Policies, ads must not promote the sale or use of weapons, ammunition, or explosives. This includes ads for weapon modification accessories. Our ad review process encompasses landing pages linked from the ad; therefore ads linking to landing pages promoting weapon sales are not allowed. More information is available at https://www.facebook.com/policies/ads/prohibited_content/weapons.

In cases where the company is clearly not solely focused on weapon sale and there are no weapons accessible on the landing page, we allow the ads. For example, a general outdoors store—if they have a diverse portfolio of products that largely don't violate our policies—can promote a backpack if they linked to an offsite landing page on which weapons are not immediately accessible.

The Honorable Mimi Walters

1. Can you please explain the difference between Ad Controls and the "privacy" controls that enable a user to determine whether a picture or post is seen by the public or just friends?

When people post on Facebook—whether in a status update or by adding information to their profiles—the ability to input the information is generally accompanied by an audience selector. This audience selector allows the person to choose who will see that piece of information on Facebook—whether they want to make the information public, share it with friends, or keep it for "Only Me." The tool remembers the audience a user shared with the last time they posted something and uses the same audience when the user shares again unless they change it. This tool appears in multiple places, such as privacy shortcuts and privacy settings. When a person makes a change to the audience selector tool in one place, the change updates the tool everywhere it appears. The audience selector also appears alongside things a user has already shared, so it's clear who can see each post. After a person shares a post, they have the option to change who it is shared with.

The audience with which someone chooses to share their information is independent of whether we use that information to personalize the ads and other content we show them. Specifically, our Data Policy explains that we may use any information that people share on Facebook "to deliver our Products, including to personalize features and content (including your News Feed, Instagram Feed, Instagram Stories and ads)." However, people can use our Ad Preferences tool to see the list of interests that we use to personalize their advertising. This means that, for example, a person who is interested in cars can continue to share that interest with their friends but tell us not to assign them an interest in ads for ad targeting purposes.

The Honorable Earl "Buddy" Carter

1. **Mr. Zuckerberg, you acknowledged at the hearing that online piracy has been a problem for quite some time. I understand that this isn't a new person or unique to your platform, but it certainly exists and needs to be addressed. Can you detail what Facebook does to prevent the use of its platform for the unlawful dissemination of content, both in terms of the hosting or transmission of the content itself, as well as the use of the platform to advertise or link to other web sites, services, and devices that are overwhelmingly engaged in piracy?**

We take intellectual property rights seriously at Facebook and work closely with the motion picture industries and other rights holders worldwide to help them protect their copyrights and other IP. Our measures target potential piracy across our products, including Facebook Live, and continue to be enhanced and expanded. These include a global notice-and-takedown program, a comprehensive repeat infringer policy, integration with the content recognition service Audible Magic, and our proprietary video- and audio-matching technology called Rights Manager. More information about these measures can be found in our Intellectual Property Help Center, Transparency Report, and Rights Manager website.

2. **Mr. Zuckerberg, you mentioned that you might use artificial intelligence to help combat not just hate speech and terrorist propaganda, but also illegal conduct, such as illicit sale of drugs, theft of intellectual property, fraud, and identity theft. Can you elaborate how Facebook is currently using AI to combat such unlawful conduct, and your plans for doing so in the future?**

We have deployed a variety of tools in the fight to find and remove content that violates our Community Standards, including artificial intelligence, specialized human review, and industry cooperation. We are more than doubling the number of people who work on safety and security at Facebook.

All content goes through some degree of automated review, and we use human reviewers to check content that has been flagged by that automated review or reported by people that use Facebook. Our content reviewers respond quickly to millions of reports each week from people all over the world. We also use human reviewers to perform reviews of content that was not flagged or reported to check the accuracy and efficiency of our automated review systems.

We respect the intellectual property rights of artists and other creators who produce copyrighted work, and we want rights holders to be able to control how their content is shared. To this end, we provide rights holders with meaningful tools for protecting their rights, including our Rights Manager video-matching technology. We also take prompt action against reported IP infringements via our global notice-and-takedown program, and we disable the accounts of repeat infringers when appropriate.

We provide rights holders with streamlined and accessible online reporting tools for submitting copyright and trademark infringement reports, and our notice-and-takedown team processes submitted reports around-the-clock. When we receive a valid notice, we work quickly to remove the reported content, and we notify both the reported party and the rights holder of the

removal. In addition, reported parties receive contact information for the rights holder in the event they want to dispute the removal, and for reports submitted under the DMCA, reported parties may submit a counter-notice.

In addition to these measures, we use systems that flag content posted to Facebook that may contain copyrighted content owned by someone else. We use Audible Magic to help prevent unauthorized videos from being posted to Facebook. Audible Magic is a third-party service that allows content owners to fingerprint their media files for copyright management. Videos uploaded to Facebook are then run through Audible Magic at the time of upload. If a match is detected, the content is rendered inaccessible to others, and the user is notified.

We also have launched Rights Manager, which is our own technology that allows copyright owners to maintain a reference library of video content they want to protect, including live video streams. Through Rights Manager, copyright owners can take a number of actions on uploaded videos that match their content. These include a block (preventing the video from being viewed by anyone other than the uploader), claiming available ad earnings, monitoring the video, or reporting the video as an IP violation.

We build and update technical systems every day to better identify and remove inauthentic accounts, which also helps reduce the distribution of material that can be spread by accounts that violate our policies. Each day, we block millions of fake accounts at registration. Our systems examine thousands of account attributes and focus on detecting behaviors that are very difficult for bad actors to fake, including their connections to others on our platform. By constantly improving our techniques, we also aim to reduce the incentives for bad actors who rely on distribution to make their efforts worthwhile.

3. Why did it take Facebook so long to ban the terms within the search function allowing illicit opioids and other drugs to be purchased through the platform? Facebook was notified this was a pervasive problem since at least as early as 2011.

We have an iterative process to help prevent opportunities for—and respond quickly to—attempts to sell illicit drugs on our platforms.

Our Community Standards and other policies make it very clear that buying, selling or trading non-medical or pharmaceutical drugs is not allowed on Facebook. Any time we become aware of content on Facebook that is facilitating activity like illicit drug sales, we remove it and have taken measures to minimize the opportunity for these activities to take place on our platform.

We make it easy for people to report any piece of content on Facebook—profiles, Pages, Groups, individual content and even comments. If we identify violating content, we are able to look for associated profiles, Pages, groups, and accounts and remove them.

We have also made it harder for people to find content that facilitates the sale of opioids on our platform.

- We have removed content that violated our policies that was surfaced in Search.

- We have filtered the search results for hundreds of terms associated with drug sales in an effort to only return links to news and non-violating information about drugs that is shared on Facebook.

- We have removed thousands of terms from being suggested in search—meaning that our systems won't recognize the beginning of the word as it is being typed and suggest what the completed term to search is.

We will continue to update our list of blocked terms as we learn of new terms bad actors may start adopting to avoid detection of their illicit activities.

We are committed to finding more ways to improve our efforts to combat the sale of illegal drugs on Facebook and we will continue to prioritize the issue this year. We recently launched a new feature on Facebook so that now, when people search for help with opioid misuse—as well as attempt to buy opioids—they are prompted with content at the top of the search results page that will ask them if they would like help finding free and confidential treatment referrals. This will then direct them to the Substance Abuse and Mental Health Services Administration National Helpline. The same resources will be available on Instagram in the coming weeks. This is one of a number of ways we are helping connect people with resources and communities to support them.

4. Which, if any, experts were consulted to help identify which controlled substances and other dangerous counterfeit medicines to flag and ban from the search function? Please describe who you worked with, or are currently working with, to combat this problem.

We consulted publicly available resources from a number of federal agencies, including the Food and Drug Administration and the National Institute on Drug Abuse. We also consulted our internal safety experts as well as our NGO partners, including Partnership for Drug Free Kids.

5. Are you currently revising your search engines to filter out and prevent people from specifically looking for, and purchasing, illicit drugs? If so, please explain the process you're using and ways you're working to prevent it from happening in the future.

See Response to Question 3.

6. A 2011 FTC finding detailed that despite Facebook's comments that people could keep their data private; it was still made public in some circumstances. Why wasn't that the catalyst for privacy changes? Why did Facebook continue to flout this policy and continue to work around the idea of 'deceptive privacy claims'?

Privacy is at the core of everything we do, and our approach to privacy starts with our commitment to transparency and control. Our threefold approach to transparency includes, first, whenever possible, providing information on the data we collect and use and how people can control it in context and in our products. Second, we provide information about how we collect and use data in our user agreements and related educational materials. And third, we enable

people to learn more about the specific data we have about them through interactive tools such as Download Your Information, which lets people download a file containing data that they may want to take to another service, and Access Your Information, a tool we are launching that will let people more easily access and manage their data on Facebook.

Our approach to control is based on the belief that people should be able to choose who can see what they share and how their data shapes their experience on Facebook. People can control the audience for their posts and the apps that can receive their data. They can see and delete the history of their activities on Facebook, and, if they no longer want to use Facebook, they can delete their account and the data associated with it. Of course, we recognize that controls are only useful if people know how to find and use them. That is why we continuously deliver in-product educational videos in people's News Feeds on important privacy topics. We are also inviting people to take our Privacy Checkup—which prompts people to review key data controls—and we are sharing privacy tips in education campaigns off of Facebook, including through ads on other websites. To make our privacy controls easier to find, we are launching a new settings menu that features core privacy settings in a single place. We are always working to help people understand and control how their data shapes their experience on Facebook.

Facebook's privacy assessments are conducted pursuant to the July 27, 2012 Consent Order. They are conducted by an independent third-party professional (PwC) pursuant to the procedures and standards generally accepted in the profession and required by the FTC, as set forth in the Consent Order. Facebook incorporated GAPP principles in designing its privacy program and related controls, which are considered industry leading principles for protecting the privacy and security of personal information. Facebook provided the FTC with summaries of these controls and engaged extensively with the FTC regarding the structure of its privacy program. Facebook has submitted copies of each assessment to the FTC.

We furnished extensive information to the FTC regarding the ability for users to port their Facebook data (including friends data that had been shared with them) with apps on Facebook's platform, as part of the FTC's investigation culminating in the July 27, 2012 Consent Order. The Consent Order memorializes the agreement between Facebook and the FTC and did not require Facebook to turn off the ability for people to port friends data that had been shared with them on Facebook to apps they used. Facebook voluntarily changed this feature of the Platform in 2014, however.

Among other things, the Consent Order obligates Facebook not to misrepresent the extent to which it maintains the privacy or security of covered information (Section I), not to materially exceed the restrictions of a privacy setting that applies to nonpublic user information without affirmative express consent (Section II), and to implement a comprehensive privacy program that is subjected to ongoing review by an independent assessor (Sections IV and V). Facebook accurately represented the operation of its developer Platform and the circumstances under which people could share data (including friends data) with developers, honored the restrictions of all privacy settings that covered developer access to data, and implemented a comprehensive privacy program built on industry-leading controls and principles, which has undergone ongoing review by an independent assessor approved by the FTC.

7. You've announced that Facebook will tell people about the misuse of their data, but that is one small sliver of activity. Why did you wait to so long to not only alert federal authorities, but also your users? Why isn't there a tool or process in place that could recognize when this happens?

When Facebook learned about Kogan's breach of Facebook's data use policies in December 2015, we took immediate action. The company retained an outside firm to assist in investigating Kogan's actions, to demand that Kogan and each party he had shared data with delete the data and any derivatives of the data, and to obtain certifications that they had done so. Because Kogan's app could no longer collect most categories of data due to changes in Facebook's platform, our highest priority at that time was ensuring deletion of the data that Kogan may have accessed before these changes took place. With the benefit of hindsight, we wish we had notified people whose information may have been impacted. Facebook has since notified all people potentially impacted with a detailed notice at the top of their News Feed.

8. There's evidence that illegal wildlife sales happen in closed groups. What is Facebook doing to remove illegal wildlife activity from the platform? Please cite examples.

We require everyone on Facebook to comply with our Community Standards. Accounts may be suspended or shut down if they violate Facebook's Terms of Service, Community Standards, or other policies.

Our Community Standards do not allow for poaching or the sale of wildlife, endangered species or their parts. This is covered under our policies for Promoting or Publicizing Crime and Coordinating Harm. As our Promoting or Publicizing Crime policy explains: we do not allow content depicting, admitting, or promoting criminal acts including "poaching or selling endangered species or their parts." As our Coordinating Harm policy explains: we do not allow statements of intent, calls to action, or advocation for acts including "poaching or selling endangered species and their parts."

We use a combination of technology, reports from our NGO partners, reports from our community and human review to remove any content that violates our policies. For instance, we use proactive detection to find and remove graphic violence. We're continuing to improve the technology to improve its ability to catch animal abuse.

In addition to our Community Standards, we also have policies prohibiting the sale of wildlife, endangered species or their parts in our Ads Policies and Commerce Policies. Our Ads policies explain "ads must not constitute, facilitate, or promote illegal products, services or activities." Our Commerce Policies prohibit the sale of animals. When it comes to violating content in ads, we review ads against our policies before they can show up on Facebook. We use a combination of automation and human review to check an ad's images and text—as well as the ad's targeting, positioning, and its landing page—to determine if the ad complies with our policies.

We also work with various NGOs and other external stakeholders to receive tips about potential violations and work with these organizations to ensure that our policies are appropriate.

We've partnered with the World Wildlife Fund on the Global Coalition to End Wildlife Trafficking Online to work with wildlife experts to combat wildlife trafficking online—https://www.worldwildlife.org/pages/global-coalition-to-end-wildlife-trafficking-online.

9. How is Facebook working with authorities in the United States, and other countries, to alert law enforcement of illegal sales? Are you willing to share this information to further combat poaching and the illegal sales of animal goods?

We have a long history of working successfully with the DOJ, the FBI, and other law enforcement to address a wide variety of threats to our platform. When appropriate, we share our understanding of abusive behavior on our platform with these authorities.

Our platform enforcement efforts involve regular contact with law enforcement authorities in the United States and around the world.

We also work with various NGOs and other external stakeholders to receive tips about potential violations and work with these organizations to ensure that our policies are appropriate. We've partnered with the World Wildlife Fund on the Global Coalition to End Wildlife Trafficking Online to work with wildlife experts to combat wildlife trafficking online—https://www.worldwildlife.org/pages/global-coalition-to-end-wildlife-trafficking-online.

10. Will you commit to working with U.S. federal law enforcement agencies to curb the presence of illegal wildlife goods on your platform?

We are saddened to hear these reports and are investigating this issue.

Our Community Standards do not allow for poaching or the sale of wildlife, endangered species or their parts, and we immediately remove this material as soon as we are aware. We have many systems in place to prevent the sale of illegal goods, and do not allow ads around the sale of endangered animals.

We have a long history of working successfully with the DOJ, the FBI, and other law enforcement to address a wide variety of threats to our platform. When appropriate, we share our understanding of abusive behavior on our platform with these authorities.

Further, we routinely respond to valid law enforcement requests for information and provide operational guidelines to law enforcement who seek records from Facebook on our site—https://www.facebook.com/safety/groups/law/guidelines/.

11. How did Facebook certify that Cambridge Analytica had deleted the data? Please describe the process of how you audit these requirements.

When Facebook learned about Kogan's breach of Facebook's data use policies in December 2015, we took immediate action. The company retained an outside firm to assist in investigating Kogan's actions, to demand that Kogan and each party he had shared data with delete the data and any derivatives of the data, and to obtain certifications that they had done so. Because Kogan's app could no longer collect most categories of data due to changes in

Facebook's platform, our highest priority at that time was ensuring deletion of the data that Kogan may have accessed before these changes took place.

In March 2018, we learned from news reports that contrary to the certifications given, not all of the Kogan data may have been deleted by Cambridge Analytica. We have no direct evidence of this and no way to confirm this directly without accessing Cambridge Analytica's systems and conducting a forensic audit. We have held off on audits of Cambridge Analytica and other parties that are being investigated by the UK Information Commissioner's Office at its request. Our investigation is ongoing.

12. Will you be overhauling your certification process for third-party apps and developers?

In April 2014, we announced that we would more tightly restrict our platform APIs to prevent abuse. At that time, we made clear that existing apps would have a year to transition—at which point they would be forced (1) to migrate to the more restricted API and (2) be subject to Facebook's new review and approval protocols. The vast majority of companies were required to make the changes by May 2015; a small number of companies (fewer than 100) were given a one-time extension of less than six months beyond May 2015 to come into compliance. (One company received an extension to January 2016.) In addition, in the context of our ongoing review of third-party apps, we discovered a very small number of companies (fewer than 10) that theoretically could have accessed limited friends' data as a result of API access that they received in the context of a beta test. We are not aware that any of this handful of companies used this access, and we have now revoked any technical capability they may have had to access any friends' data.

New apps that launched after April 30, 2014 were required to use our more restrictive platform APIs. We required apps seeking additional categories of data to undergo proactive review by our internal teams. We rejected more than half of the apps seeking these permissions, including the second version of Kogan's app.

We review apps to ensure that the requested permissions clearly improve the user experience and that the data obtained is tied to an experience within the app. We conduct a variety of manual and automated checks of applications on the platform for Policy compliance, as well as random sampling. When we find evidence of or receive allegations of violations, we investigate and, where appropriate, employ a number of measures, including restricting applications from our platform, preventing developers from building on our platform in the future, and taking legal action where appropriate.

Recently, we announced a number of additional steps we're taking to address concerns raised by Kogan's app.

- **Review our platform.** We will investigate all apps that had access to large amounts of data before the platform changes we announced in 2014, and we will audit any app where we identify suspicious activity. If we identify misuses of data, we'll take immediate action, including banning the app from our platform and pursuing legal action if appropriate.

- **Tell people about data misuse.** We will tell people about apps that have misused their data.

- **Turn off access for unused apps.** If someone has not used an app within the last three months, we will turn off the app's access to their data.

- **Restrict Facebook Login data.** We are changing Login, so that the only data that an app can request without app review will include name, profile photo, and email address. Requesting any other data will require approval from Facebook. We will also no longer allow apps to ask for access to information like religious or political views, relationship status and details, custom friends lists, education and work history, fitness activity, book reading and music listening activity, news reading, video watch activity, and games activity. We will encourage people to manage the apps they use. We already show people what apps their accounts are connected to and allow them to control what data they've permitted those apps to use. But we're making it easier for people to see what apps they use and the information they have shared with those apps.

- **Reward people who find vulnerabilities.** We launched the Data Abuse Bounty program so that people can report to us any misuses of data by app developers.

- **Update our policies.** We have updated our terms and Data Policy to explain how we use data and how data is shared with app developers.

13. Facebook announced they were changing their search by phone and email functions as well the account recovery system after you found malicious groups were using this vulnerability to attain user data. I understand you believe all users could have their data scraped this way. Why wasn't this information relayed to the public?

In April, we found out that a feature that lets users look someone up by their phone number and email may have been misused by browsers looking up people's profiles in large volumes with phone numbers they already had. When we found out about the abuse, we shut this feature down. In the past, we have been aware of scraping as an industry issue, and have dealt with specific bad actors previously. We informed the public through this post: https://newsroom.fb.com/news/2018/04/restricting-data-access/.

14. Differential privacy is a tool that takes the information of its users and disaggregates it so that they can utilize data trends, but can't extract data about any specific users. This ensures they get the most of out of the data collection on user trends but doesn't allow for individually-identifiable information. This tech not only reduces their liability, but also prevents others from utilizing the information if breached. Does Facebook have any plans to fully anonymize the data gleaned from its users, like differential privacy, to prevent personally-identifiable information from being used for improper purposes?

We're constantly working on new ways to leverage privacy-preserving technologies for our products and data infrastructure. We use various techniques, including differential privacy, to

de-identify data where possible. We also have many different systems in place that monitor how data is used to prevent it from being used improperly.

15. Will you be changing the data collection methods that can be used by academic authorities?

We disclose our work with academic researchers in our Data Policy, and our work with academics is conducted subject to strict privacy and research protocols.

16. Cambridge Analytica garnered the majority of their user information from friends of the users who participated in the app. Has Facebook changed its policy that would allow friends to have their profiles scraped of information?

See Response to Question 12.

The Honorable Frank Pallone, Jr.

1. At the House hearing, I asked some questions about Facebook's practices regarding its own collection and use of people's data. You seemed to misunderstand my questions, so I'm asking them again to get better answers from you.

a. Between February 17, 2018, and the hearing on April 11, 2018, Facebook made a number of announcements about changes it was making in response to the news of the Cambridge Analytica incident. Yes or no, did any of those changes include new limitations on the amount or type of data Facebook itself collects or uses?

Recently, we announced a number of additional steps we're taking to address concerns raised by Kogan's app.

- **Review our platform.** We will investigate all apps that had access to large amounts of data before the platform changes we announced in 2014, and we will audit any app where we identify suspicious activity. If we identify misuses of data, we'll take immediate action, including banning the app from our platform and pursuing legal action if appropriate.

- **Tell people about data misuse.** We will tell people about apps that have misused their data.

- **Turn off access for unused apps.** If someone has not used an app within the last three months, we will turn off the app's access to their data.

- **Restrict Facebook Login data.** We are changing Login, so that the only data that an app can request without app review will include name, profile photo, and email address. Requesting any other data will require approval from Facebook. We will also no longer allow apps to ask for access to information like religious or political views, relationship status and details, custom friends lists, education and work history, fitness activity, book reading and music listening activity, news reading, video watch activity, and games activity. We will encourage people to manage the apps they use. We already show people what apps their accounts are connected to and allow them to control what data they've permitted those apps to use. But we're making it easier for people to see what apps they use and the information they have shared with those apps.

- **Reward people who find vulnerabilities.** We launched the Data Abuse Bounty program so that people can report to us any misuses of data by app developers.

- **Update our policies.** We have updated our terms and Data Policy to explain how we use data and how data is shared with app developers.

b. At the hearing, I asked you whether Facebook was changing any user default settings to be more privacy protective. In response, you stated "we have changed a lot of the way that our platform works so that way developers

can't get access to as much information." But I was asking about default settings related to the amount and type of data Facebook itself collects and uses, not what third parties have access to. So I will ask again. Yes or no, has Facebook changed any default privacy settings to be more privacy protective with regard to the amount and type of information Facebook itself collects and uses?

We regularly review and update our settings to help people protect their privacy and give people choices about how their information is used and who can see it. That's why, for example, in 2014 we changed the default audience for posts from Public to Friends, and why we now ask people when they create a new account who they would like to see the things they post—their friends, the public, or a different audience.

c. At the hearing, you would not commit to making all the user default settings to minimize to the greatest extent possible the collection and use of user's data. I am giving you another chance to make that commitment. Yes or no, will you commit to changing all the user default settings to minimize to the greatest extent possible the collection and use of users' data? If you cannot make that commitment, why not?

Privacy is at the core of everything we do, and our approach to privacy starts with our commitment to transparency and control. Our threefold approach to transparency includes, first, whenever possible, providing information on the data we collect and use and how people can control it in context and in our products. Second, we provide information about how we collect and use data in our user agreements and related educational materials. And third, we enable people to learn more about the specific data we have about them through interactive tools such as Download Your Information, which lets people download a file containing data that they may want to take to another service, and Access Your Information, a tool we are launching that will let people more easily access and manage their data on Facebook.

Our approach to control is based on the belief that people should be able to choose who can see what they share and how their data shapes their experience on Facebook. People can control the audience for their posts and the apps that can receive their data. They can see and delete the history of their activities on Facebook, and, if they no longer want to use Facebook, they can delete their account and the data associated with it. Of course, we recognize that controls are only useful if people know how to find and use them. That is why we continuously deliver in-product educational videos in people's News Feeds on important privacy topics. We are also inviting people to take our Privacy Checkup—which prompts people to review key data controls—and we are sharing privacy tips in education campaigns off of Facebook, including through ads on other websites. To make our privacy controls easier to find, we are launching a new settings menu that features core privacy settings in a single place. We are always working to help people understand and control how their data shapes their experience on Facebook.

We recognize, however, that controls are only useful if people know how to find and use them. That is why we continuously deliver in-product educational videos in people's News Feeds on important privacy topics like how to review and delete old posts and what it means to delete an account. We are also inviting people to take our Privacy Checkup—which prompts people to

review key data controls—and we are sharing privacy tips in education campaigns off of Facebook, including through ads on other websites. To make our privacy controls easier to find, we are launching a new settings menu that features core privacy settings in a single place.

2. At both the Senate and House hearings, you noted multiple times that Facebook users have controls over their data and they can choose with whom they want to share their data. In response to a question from Congressman Rush about default privacy settings, you again noted that whenever a Facebook user posts something, they can choose who they share that posting with through a control right where they are posting the particular content.

a. When a user posts, say, a photo and chooses to share with "friends only," how does Facebook use that information? Is it incorporated into a user's interests for advertising purposes in any way?

b. When a user "likes" another user's post, what options does the user have to control who sees the like? How does Facebook use that information? Is it incorporated into a user's interests for advertising purposes in any way?

c. When a user posts a comment on another user's post, what options does the user have to control who sees the comment? How does Facebook use that information? Is it incorporated into a user's interests for advertising purposes in any way?

d. When a user posts a comment or likes a post from a Page, what options does the user have to control who sees the comment or like? How does Facebook use that information? Is it incorporated into a user's interests for advertising purposes in any way?

e. When a user posts a comment or likes a post from an advertiser, what options does the user have to control who sees the comment or like? How does Facebook use that information? Is it incorporated into a user's interests for advertising purposes in any way?

When people post on Facebook—whether in a status update or by adding information to their profiles—the ability to input the information is generally accompanied by an audience selector. This audience selector allows the person to choose who will see that piece of information on Facebook—whether they want to make the information public, share it with friends, or keep it for "Only Me." The tool remembers the audience a user shared with the last time they posted something and uses the same audience when the user shares again unless they change it. This tool appears in multiple places, such as privacy shortcuts and privacy settings. When a person makes a change to the audience selector tool in one place, the change updates the tool everywhere it appears. The audience selector also appears alongside things a user has already shared, so it's clear who can see each post. After a person shares a post, they have the option to change who it is shared with.

The audience with which someone chooses to share their information is independent of whether we use that information to personalize the ads and other content we show them. Specifically, our Data Policy explains that we may use any information that people share on Facebook "to deliver our Products, including to personalize features and content (including your News Feed, Instagram Feed, Instagram Stories and ads)." However, people can use our Ad Preferences tool to see the list of interests that we use to personalize their advertising. This means that, for example, a person who is interested in cars can continue to share that interest with their friends but tell us not to assign them an interest in ads for ad targeting purposes.

3. There has been a lot reported in the press about the Cambridge Analytica scandal and there is confusion about who exactly has access to the data collected by Aleksandr Kogan. I do not think the American people know how much of their data Facebook carelessly made available to anyone with the wherewithal to get it. And I do not think you even know how much Facebook user information is out there.

a. Yes or no, you do not actually know who or even how many people or entities have the user data that Cambridge Analytica had obtained from Aleksandr Kogan?

On December 11, 2015, *The Guardian* published an article reporting that Kogan and his company, GSR, may have passed information the app had obtained from Facebook users to SCL Elections Ltd. (SCL)/Cambridge Analytica. Kogan and his company violated Facebook's Platform Policies, which explicitly prohibited selling user data accessed from Facebook and from sharing any user data accessed from Facebook with any ad network, data broker or other advertising or monetization related service.

For this reason, Facebook immediately banned the app from our platform and investigated what happened and what further action we should take to enforce our Platform Policies. Facebook also contacted Kogan/GSR and demanded that they explain what data they collected, how they used it, and to whom they disclosed it. Facebook further insisted that Kogan and GSR, as well as other persons or entities to whom they had disclosed any such data, account for and irretrievably delete all such data and information.

Facebook also contacted Cambridge Analytica to investigate the allegations reflected in the reporting. On January 18, 2016, Cambridge Analytica provided written confirmation to Facebook that it had deleted the data received from Kogan and that its server did not have any backups of that data. On June 11, 2016, Kogan executed signed certifications of deletion on behalf of himself and GSR. The certifications also purported to identify all of the individuals and entities that had received data from GSR (in addition to Kogan and his lab), listing the following: SCL, Eunoia Technologies (a company founded by Christopher Wylie), and a researcher at the Toronto Laboratory for Social Neuroscience at the University of Toronto. On July 7, 2016, a representative of the University of Toronto certified that it deleted any user data or user-derived data. On August 16, 2016, Eunoia (executed by Eunoia Founder Christopher Wylie) certified that it deleted any user and user-derived data. On September 6, 2016, counsel for SCL informed counsel for Facebook that SCL had permanently deleted all Facebook data and derivative data received from GSR and that this data had not been transferred or sold to any other entity. On

April 3, 2017, Alexander Nix, on behalf of SCL, certified to Facebook, that it deleted the information that it received from GSR or Kogan.

Because all of these concerns relate to activity that took place off of Facebook and its systems, we have no way to confirm whether Cambridge Analytica may have Facebook data without conducting a forensic audit of its systems. Cambridge Analytica has agreed to submit to a forensic audit, but we have not commenced that yet due to a request from the UK Information Commissioner's Office, which is simultaneously investigating Cambridge Analytica (which is based in the UK). And even with an audit, it may not be possible to determine conclusively what data was shared with Cambridge Analytica or whether it retained data after the date it certified that data had been deleted.

The existing evidence that we are able to access supports the conclusion that Kogan only provided SCL with data on Facebook users from the United States. While the accounts of Kogan and SCL conflict in some minor respects not relevant to this question, both have consistently maintained that Kogan never provided SCL with any data for Facebook users outside the United States. These consistent statements are supported by a publicly released contract between Kogan's company and SCL.

b. Yes or no, you do not actually know how many other "Cambridge Analyticas" that are out there—that is, entities that may not have had a direct relationship with Facebook that got Facebook user data through some improper means?

We are in the process of investigating every app that had access to a large amount of information before we changed our Platform in 2014. The investigation process is in full swing, and it has two phases. First, a comprehensive review to identify every app that had access to this amount of Facebook data and to focus on apps that present reason for deeper investigation. And second, where we have concerns, we will conduct interviews, make requests for information (RFI)—which ask a series of detailed questions about the app and the data it has access to—and perform audits using expert firms that may include on-site inspections. We have large teams of internal and external experts working hard to investigate these apps as quickly as possible. As of early June 2018, thousands of apps have been investigated and around 200 apps have been suspended—pending a thorough investigation into whether they did in fact misuse any data. Where we find evidence that these or other apps did misuse data, we will ban them and let people know.

These apps relate to a handful of developers: Kogan, AIQ, Cube You, the Cambridge Psychometrics Center, and myPersonality, with many of the suspended apps being affiliated with the same entity. Many of these suspensions include apps that appear to be "test" apps that were never released to the public, and therefore would not have acquired significant user data, although our investigation into these apps is ongoing.

Additionally, we have suspended an additional 14 apps, which were installed by around one thousand people. They were all created after 2014, after we made changes to more tightly restrict our platform APIs to prevent abuse. However, these apps appear to be linked to AIQ,

which was affiliated with Cambridge Analytica. So, we have suspended them while we investigate further. Any app that refuses to take part in or fails our audit will be banned.

We will commit to briefing your staff on future developments.

c. How many app developers accessed friends' data in the years that information was made available to them?

See the response to Question 3(b).

4. Following the FTC consent decree in 2011, while friends' data was available to app developers, did Facebook transmit to app developers the friends' privacy choices. For example, if a friend who was not the person who downloaded the app set her privacy settings for, say, her phone number to "friends only," did Facebook communicate that choice to the app developers? Did Facebook automatically block that information from being shared with the app at all?

We furnished extensive information to the FTC regarding the ability for users to port their Facebook data (including friends data that had been shared with them) with apps on Facebook's platform, as part of the FTC's investigation culminating in the July 27, 2012 Consent Order. The Consent Order memorializes the agreement between Facebook and did not require Facebook to turn off the ability for people to port friends data that had been shared with them on Facebook to apps they used. Facebook voluntarily changed this feature of the Platform in 2014, however.

In 2011, Facebook offered more control and protection over the availability of friends data to apps than any other digital platform at the time, including mobile app platforms, which generally permitted apps to access user data and their friends' data without consent or any control. By contrast, Facebook notified users of each category of data an app could access—including friends data—before the user consented to the app, and also provided all users with controls that would prevent their friends from sharing their data with apps on Facebook's platform.

In November 2013, when Kogan launched his app, apps generally could be launched on the Platform without affirmative review or approval by Facebook. The app used the Facebook Login service, which allowed users to utilize their Facebook credentials to authenticate themselves to third-party services. Facebook Login and Facebook's Graph API also allowed the app to request permission from its users to bring their Facebook data (their own data and data shared with them by their friends) to the app, to obtain new experiences.

At that time, the Graph API V1 allowed app developers to request consent to access information from the installing user such as name, gender, birthdate, location (i.e., current city or hometown), photos and Page likes—and also (depending on, and in accordance with, each friend's own privacy settings) the same or similar categories of information the user's friends had shared with the installing user. Permitting users to share data made available to them by their friends had the upside of making the experience of app users more personalized and social. For example, a Facebook user might want to use a music app that allowed the user to (1) see what his

or her friends were listening to and (2) give the app permission to access the user's friend list and thereby know which of the user's friends were also using the app. Such access to information about an app user's friends required not only the consent of the app user, but also required that the friends whose data would be accessed have their own privacy settings set to permit such access by third-party apps. In other words, Kogan's app could have accessed a user's friends' information only for friends whose privacy settings permitted such sharing.

In April 2014, we announced that we would more tightly restrict our platform APIs to prevent abuse. At that time we made clear that existing apps would have a year to transition—at which point they would be forced (1) to migrate to the more restricted API and (2) be subject to Facebook's new review and approval protocols. The vast majority of companies were required to make the changes by May 2015. The following small set of companies (fewer than 100) were given a one-time extension of less than six months beyond May 2015 to come into compliance. (One company, Serotek, an accessibility app, received an 8 months extension to January 2016.)

1. ABCSocial, ABC Television Network
2. Actiance
3. Adium
4. Anschutz Entertainment Group
5. AOL
6. Arktan / Janrain
7. Audi
8. biNu
9. Cerulean Studios
10. Coffee Meets Bagel
11. DataSift
12. Dingtone
13. Double Down Interactive
14. Endomondo
15. Flowics, Zauber Labs
16. Garena
17. Global Relay Communications
18. Hearsay Systems
19. Hinge
20. HiQ International AB
21. Hootsuite
22. Krush Technologies
23. LiveFyre / Adobe Systems
24. Mail.ru
25. MiggoChat
26. Monterosa Productions Limited
27. never.no AS
28. NIKE
29. Nimbuzz
30. NISSAN MOTOR CO / Airbiquity Inc.
31. Oracle
32. Panasonic

33. Playtika
34. Postano, TigerLogic Corporation
35. Raidcall
36. RealNetworks, Inc.
37. RegED / Stoneriver RegED
38. Reliance/Saavn
39. Rovi
40. Salesforce/Radian6
41. SeaChange International
42. Serotek Corp.
43. Shape Services
44. Smarsh
45. Snap
46. Social SafeGuard
47. Socialeyes LLC
48. SocialNewsdesk
49. Socialware / Proofpoint
50. SoundayMusic
51. Spotify
52. Spredfast
53. Sprinklr / Sprinklr Japan
54. Storyful Limited / News Corp
55. Tagboard
56. Telescope
57. Tradable Bits, TradableBits Media Inc.
58. UPS
59. Vidpresso
60. Vizrt Group AS
61. Wayin

In addition, in the context of our ongoing review of third-party apps, we discovered a very small number of companies (fewer than 10) in the following list that theoretically could have accessed limited friends' data as a result of API access that they received in the context of a beta test. We are not aware that any of this handful of companies used this access, and we have now revoked any technical capability they may have had to access any friends' data.

1. Activision / Bizarre Creations
2. Fun2Shoot
3. Golden Union Co.
4. IQ Zone / PicDial
5. PeekSocial

It is important to note that the lists above are comprehensive to the best of our ability. It is possible we have not been able to identify some extensions. It is also possible that early records may have been deleted from our system.

New apps that launched after April 30, 2014 were required to use our more restrictive platform APIs, which incorporated several key new elements, including:

- Institution of a review and approval process, called App Review (also called Login Review), for any app seeking to operate on the new platform that would request access to data beyond the user's own public profile, email address, and a list of friends of the user who had installed and authorized the same app;

- Generally preventing new apps on the new platform from accessing friends data without review; and

- Providing users with even more granular controls over their permissions as to what categories of their data an app operating on the new platform could access.

The App Review process introduced in 2014 required developers who create an app that asks for more than certain basic user information to justify the data they are looking to collect and how they are going to use it. Facebook then reviewed whether the developer has a legitimate need for the data in light of how the app functions. Only if approved following such review can the app ask for a user's permission to get their data. Facebook has rejected more than half of the apps submitted for App Review between April 2014 and April 2018, including Kogan's second app. We are changing Login so that the only data that an app can request without app review will include name, profile photo, and email address.

5. At the House hearing on April 11, 2018, you told Congressman Engel that you would follow up with new AI tools Facebook is deploying "that can proactively catch fake accounts that Russia or others might create to spread misinformation."

a. Please describe in detail these new tools and how they work.

b. You also mentioned at the hearing that Facebook was able to deploy those new tools in the French Presidential election, the German election, and in the Alabama special election for U.S. Senate to take down "tens of thousands" of fake accounts that may have been trying to influence those elections.

i For each of those three elections, how many total fake accounts may have been trying to influence the election? What percentage of fake accounts were Facebook's AI tools able to identify?

ii For each of those three elections, how many accounts were identified as fake by those AI tools that were not actually fake?

iii For each of those three elections, how many accounts were identified as fake that were not taken down before the election? When were they identified? By what method were they identified, e.g., through a report from a user or by the use of AI tools?

c. What steps other than AI is Facebook taking to proactively identify fake accounts?

Stopping this type of abuse is a focus for many teams, some more directly and some in more of a supportive role. For example, in addition to developing our AI, we are also expanding our threat intelligence team, and more broadly, we are working now to ensure that we will more than double the number of people working on safety and security at Facebook, from 10,000 to 20,000, by the end of 2018. We expect to have at least 250 people specifically dedicated to safeguarding election integrity on our platforms, and that number does not include the thousands of people who will contribute to this effort in some capacity. Many of the people we are adding to these efforts will join our ad review team, and we also expect to add at least 3,000 people to Community Operations, which reviews content that our users and automated tools flag as inappropriate, dangerous, abusive, or otherwise violating our policies. We publish information and metrics about fake accounts at https://transparency.facebook.com/community-standards-enforcement#fake-accounts and in our quarterly SEC filings.

6. After being asked by multiple members about the information contained in the document available through Facebook's Download Your Information tool, you corrected the record to note that web logs are not included in Download Your Information but that those web logs are converted into a set of ad interests that are included in the document.

a. Do those web logs include websites users visit when they are logged out of Facebook?

b. Please explain in detail the process by which web logs are converted to ad interests. Are algorithms used for that conversion? If so, please detail how those algorithms work. Use examples if necessary.

c. You said that Facebook stores web logs temporarily. Exactly how long are web logs stored on Facebook's servers?

d. Yes or no, can a Facebook user opt out of having their web log collected at all?

e. Yes or no, can a Facebook user opt out of having their web log converted to ad interests?

f. Please list in detail all the categories of information that are collected by Facebook for any purpose but that are not included in the document produced by the Download Your Information tool.

g. Please list in detail all categories of information obtained by third parties for any purpose but that are not included in the document produced by the Download Your Information tool.

Our Download Your Information or "DYI" tool is Facebook's data portability tool and was launched many years ago to let people access and download many types of information that we maintain about them. The data in DYI and in our Ads Preferences tool contain each of the interest categories that are used to show people ads, along with information about the advertisers that are currently running ads based on their use of an advertiser's website or app. People also

can choose not to see ads from those advertisers. We recently announced expansions to Download Your Information, which, among other things, will make it easier for people to see their data, delete it, and easily download and export it. More information is available at https://newsroom.fb.com/news/2018/04/new-privacy-protections.

Responding to feedback that we should do more to provide information about websites and apps that send us information when people use them, we also announced plans to build Clear History. This new feature will enable users to see the websites and apps that send us information when they use them, clear this information from their account, and turn off Facebook's ability to store it associated with their account going forward.

We have also introduced Access Your Information. This feature provides a new way for people to access and manage their information. Users can go here to delete anything from their timeline or profile that they no longer want on Facebook. They can also see their ad interests, as well as information about ads they've clicked on and advertisers who have provided us with information about them that influence the ads they see. From here, they can go to their ad settings to manage how this data is used to show them ads.

7. You mentioned many times at both the House and Senate hearings on April 10-11, 2018, that Facebook users control all the data they put into Facebook. But we know that Facebook has information about users that those users did not "put in," such as photos of users posted by Facebook friends or web logs.

a. Please detail all categories of information that Facebook collects or stores about users Facebook considers as information provided by users, such as metadata contained in a photo.

b. Please detail all categories of information that Facebook collects or stores about users that are not information Facebook users directly "put in" themselves.

c. Please detail how users can opt out of allowing Facebook to collect or store information not directly provided by users. Please also detail how users can opt out of allowing Facebook to collect or store information considered as information provided by users, such as metadata contained in photos.

d. In response to a question from Congresswoman Matsui, you stated that Facebook "use[s] the data that people put into the system in order to make the ads more relevant, which also makes them more valuable." Do you only use data people "put into" the system to make the ads more relevant or do you also use other information, such as web logs, to make ads more relevant?

e. You also responded to Congresswoman Matsui that users have "complete control" over advertising data. Please explain in detail the ways in which users can control the data used for advertising purposes, including information that users did not put directly into Facebook's systems. How can users delete the information used for advertising purposes, including

information that users did not put directly into Facebook's systems themselves?

As explained in our Data Policy, we collect three basic categories of data about people: (1) data about things people do and share (and who they connect with) on our services, (2) data about the devices people use to access our services, and (3) data we receive from partners, including the websites and apps that use our business tools.

Our Data Policy provides more detail about each of the three categories. Any person can see each of the specific interests we maintain about them for advertising by visiting Ads Preferences, which lets people see what interests we use to choose ads for them—and to edit or delete these interests.

We use data from each of the categories described above to obtain these interests and to personalize every aspect of our services, which is the core value we offer and the thing that makes Facebook services unique from other online experiences. This includes selecting and ranking relevant content, including ads, posts, and Page recommendations, to cite but a few examples.

For example, we use the data people provide about their age and gender to help advertisers show ads based on those demographics but also to customize the pronouns on our site and deliver relevant experiences to those users.

We use data about things people do on Facebook, such as the Pages they like, to associate "interests" with their accounts, so we can rank posts relating to those interests higher in News Feed, for example, or enable advertisers to reach audiences—i.e., groups of people—that share those interests. For example, if a person has liked Pages about baseball, we might associate them with interests called "baseball" or "sports."

We use data from devices (such as location data) to help advertisers reach people in particular areas. For example, if people have shared their device locations with Facebook or checked into a specific restaurant, we can show them organic posts from friends who have been in that location or we can show them ads from an advertiser that wants to promote its services in their area or from the restaurant.

We also help advertisers reach people who have given the advertiser their contact information or who have used the advertiser's website or app. For example, advertisers can send us a hashed list of email addresses of people they would like to reach on Facebook. If we have matching email addresses, we can show those people ads from that advertiser (although we cannot see the email addresses which are sent to us in hashed form, and these are deleted as soon as we complete the match).

As far as the amount of data we collect about people, the answer depends on the person. People who have only recently signed up for Facebook have usually shared only a few things—such as name, contact information, age, and gender. Over time, as people use our products, we receive more data from them, and this data helps us provide more relevant content and services. That data will fall into the categories noted above, but the specific data we receive will, in large part, depend on how the person chooses to use Facebook. For example, some people use

Facebook to share photos, so we receive and store photos for those people. Some people enjoy watching videos on Facebook; when they do, we receive information about the video they watched, and we can use that information to help show other videos in their News Feeds. Other people seldom or never watch videos, so we do not receive the same kind of information from them, and their News Feeds are likely to feature fewer videos.

The data we have about people also depends on how they have used our controls. For example, people who share photos can easily delete those photos. The same is true of any other kind of content that people post on our services. Through Facebook's Activity Log tool, people can also control the information about their engagement—i.e., their likes, shares and comments—with other people's posts. The use of these controls of course affects the data we have about people.

We recently announced improvements to our Download Your Information tool, as well as a new feature that makes it easier for people to see the information that's in their account on Facebook. These recently-expanded tools for accessing your information will allow people to see their data, delete it, and easily download and export it.

We also provide controls that specifically govern the use of data for ads. Through Ad Preferences, people see and control things like: (1) their "interests," which are keywords associated with a person based on activities such liking Pages and clicking ads; (2) their "behaviors" (which we also call "categories"), which generally reflect how, when and where they connect to Facebook; and (3) the advertisers that are currently showing them ads based on the person's contact information, based on the person's previous use of the advertiser's website or app, or based on a visit to the advertiser's store. People also can choose whether we use information about their activities on websites and apps off of Facebook to show them ads through Facebook, and whether we can use their Facebook advertising interests to show them ads off of Facebook. People's use of these controls will, of course, affect the data we use to show them ads.

8. At the House hearing, Congresswoman Castor asked you to confirm that Facebook collects medical data on people that are not on the Internet, whether they are Facebook users or not. You confirmed that Facebook does "collect some data for security purposes."

a. Explain exactly how medical information collected offline is used for security purposes. What other ways and for what other purposes could medical data collected offline be used by Facebook?

b. Please detail all categories of information Facebook collects for security purposes, and identify whether that information is collected about Facebook users, nonusers, or both.

c. Please explain in detail how that data is used for security purposes.

d. Is any such data used for purposes other than security purposes? If so, please describe all other ways such data is used?

We understand you to be asking about research discussions Facebook had with medical institutions. Facebook was exploring this type of data sharing because of the general health benefits to having a close-knit circle of family and friends and the need for more research on the impact of social connection on health. Deeper research into this link is needed to help medical professionals develop specific treatment and intervention plans that take social connection into account. With this in mind, last year Facebook began discussions with leading medical institutions, including the American College of Cardiology and the Stanford University School of Medicine, to explore whether scientific research using fully-anonymized Facebook data could help the medical community advance our understanding in this area. This work did not progress past the planning phase, and we have not received, shared, or analyzed anyone's data.

In March we decided that we should pause these discussions so we can focus on other important work, including doing a better job of protecting people's data and being clearer with them about how that data is used in our products and services.

Our Data Policy has explained that we have engaged in research collaborations for several years. As part of a general effort to be more transparent, we updated our Data Policy recently to provide additional detail on a range of practices, including academic research. We also explain this in other ways, including announcements in our Newsroom and in a dedicated website providing more information about research at Facebook.

We use several types of data for security purposes. For example, when people visit apps or websites that feature our technologies—like the Facebook Like or Comment button—our servers automatically log (i) standard browser or app records of the fact that a particular device or user visited the website or app (this connection to Facebook's servers occurs automatically when a person visits a website or app that contains our technologies, such as a Like button, and is an inherent function of internet design); and (ii) any additional information the publisher of the app or website chooses to share with Facebook about the person's activities on that site (such as the fact that a purchase was made on the site). This is a standard feature of the internet, and most websites and apps share this same information with multiple different third-parties whenever people visit their website or app. We use the browser and app logs that apps and websites send to us in the following ways for non-Facebook users. First, these logs are critical to protecting the security of Facebook and to detecting or preventing fake account access. For example, if a browser has visited hundreds of sites in the last five minutes, that's a sign the device might be a bot, which would be an important signal of a potentially inauthentic account if that browser then attempted to register for an account. Second, we aggregate those logs to provide summaries and insights to websites and apps about how many people visit or use their product, or use specific features like our Like button—but without providing any information about a specific person. We do not create profiles for non-Facebook users, nor do we use browser and app logs for non-Facebook users to show targeted ads from our advertisers to them or otherwise seek to personalize the content they see. However, we may take the opportunity to show a general ad that is unrelated to the attributes of the person or an ad encouraging the non-user to sign up for Facebook.

When the individual is a Facebook user, we are also able to use this information to personalize their experiences on Facebook, whether or not they are logged out, but we will not target ads to users relying on this information unless the user allows this in their privacy settings.

We do not sell or share this information with third-parties. Further, the same core data sets are used to ensure the safety and security of our platform and to provide our core service to our users.

9. In response to questions from Congressman Lujan at the House hearing, you noted that Facebook collects information from people who have not signed up for Facebook for security purposes.

a. Congressman Lujan asked a couple of questions that you were not able to answer at the hearing, so I would like to get those answers from you on the record.

i How many data points does Facebook have on the average Facebook user?

ii How many data points does Facebook have on the average non-Facebook user?

b. Please detail all categories of information Facebook collects from and about non- Facebook users for any purpose.

c. Please explain in detail how data collected from and about non-Facebook users are used for security purposes.

d. Please detail how Facebook uses data collected from and about non-Facebook users for purposes other than security purposes. Are such data used in any way for advertising purposes? Please explain.

e. Please identify the website or pop-up or any place where those people who have never signed up for a Facebook account have consented to allow Facebook to collect information about them.

f. Please describe in detail how a person who does not have a Facebook account can opt out of Facebook's involuntary data collection or get the information Facebook has stored about them deleted from Facebook's servers.

As explained in our Data Policy, we collect three basic categories of data about people: (1) data about things people do and share (and who they connect with) on our services, (2) data about the devices people use to access our services, and (3) data we receive from partners, including the websites and apps that use our business tools. Our Data Policy provides more detail about each of the three categories.

As far as the amount of data we collect about people, the answer depends on the person. People who have only recently signed up for Facebook have usually shared only a few things—such as name, contact information, age, and gender. Over time, as people use our products, we receive more data from them, and this data helps us provide more relevant content and services. That data will fall into the categories noted above, but the specific data we receive will, in large part, depend on how the person chooses to use Facebook. For example, some people use

Facebook to share photos, so we receive and store photos for those people. Some people enjoy watching videos on Facebook; when they do, we receive information about the video they watched, and we can use that information to help show other videos in their News Feeds. Other people seldom or never watch videos, so we do not receive the same kind of information from them, and their News Feeds are likely to feature fewer videos.

The data we have about people also depends on how they have used our controls. For example, people who share photos can easily delete those photos. The same is true of any other kind of content that people post on our services. Through Facebook's Activity Log tool, people can also control the information about their engagement—i.e., their likes, shares and comments—with other people's posts. The use of these controls of course affects the data we have about people.

When people visit apps or websites that feature our technologies—like the Facebook Like or Comment button—our servers automatically log (i) standard browser or app records of the fact that a particular device or user visited the website or app (this connection to Facebook's servers occurs automatically when a person visits a website or app that contains our technologies, such as a Like button, and is an inherent function of internet design); and (ii) any additional information the publisher of the app or website chooses to share with Facebook about the person's activities on that site (such as the fact that a purchase was made on the site). This is a standard feature of the internet, and most websites and apps share this same information with multiple different third-parties whenever people visit their website or app. For example, the House Energy and Commerce Committee's website shares information with Google Analytics to help improve the site. This means that, when a person visits the Committee's website, it sends browser information about their visit to that third party. More information about how this works is available at https://newsroom.fb.com/news/2018/04/data-off-facebook/. We require websites and apps who use our tools to tell users they're collecting and sharing their information with us, and to get users' permission to do so.

We use the browser and app logs that apps and websites send to us—described above—in the following ways for non-Facebook users. First, these logs are critical to protecting the security of Facebook and to detecting or preventing fake account access. For example, if a browser has visited hundreds of sites in the last five minutes, that's a sign the device might be a bot, which would be an important signal of a potentially inauthentic account if that browser then attempted to register for an account. Second, we aggregate those logs to provide summaries and insights to websites and apps about how many people visit or use their product, or use specific features like our Like button—but without providing any information about a specific person. We do not create profiles for non-Facebook users, nor do we use browser and app logs for non-Facebook users to show targeted ads from our advertisers to them or otherwise seek to personalize the content they see. However, we may take the opportunity to show a general ad that is unrelated to the attributes of the person or an ad encouraging the non-user to sign up for Facebook.

When the individual is a Facebook user, we are also able to use this information to personalize their experiences on Facebook, whether or not they are logged out, but we will not target ads to users relying on this information unless the user allows this in their privacy settings. We do not sell or share this information with third-parties.

We do receive some information from devices and browsers that may be used by non-users. For example:

- We also may receive information about the device of a non-registered user if that user visits a part of Facebook that does not require people to log in—such as a public Facebook Page. The information we log when people visit our websites or apps is the same as described above and is the same information that any provider of an online service would receive.

- In addition, Facebook may receive some basic information about devices where Facebook apps are installed, including before people using those devices have registered for Facebook (such as when a user downloads a Facebook app, but has not yet created an account, or if the app is preloaded on a given device). This device data includes things like device model, operating system, IP address, app version and device identifiers. We use this information to provide the right version of the app, help people who want to create accounts (for example, optimizing the registration flow for the specific device), retrieving bug fixes and measuring and improving app performance. We do not use this information to build profiles about non-registered users.

We recently announced plans to introduce Clear History, a new feature that will enable users to see the websites and apps that send us information when they use them, clear this information from their accounts, and turn off our ability to store it associated with their accounts going forward.

Apps and websites that use features such as the Like button or Facebook Analytics send us information to make their content and ads better. We also use this information to make user experience on Facebook better. If a user clears his or her history or uses the new setting, we'll remove identifying information so a history of the websites and apps the user used won't be associated with the user's account. We'll still provide apps and websites with aggregated analytics—for example, we can build reports when we're sent this information so we can tell developers if their apps are more popular with men or women in a certain age group. We can do this without storing the information in a way that's associated with the user's account, and as always, we don't tell advertisers who users are.

It will take a few months to build Clear History. We'll work with privacy advocates, academics, policymakers, and regulators to get their input on our approach, including how we plan to remove identifying information and the rare cases where we need information for security purposes. We've already started a series of roundtables in cities around the world and heard specific demands for controls like these at a session we held at our headquarters. We're looking forward to doing more.

If a person doesn't have a Facebook account but believes Facebook may have information about them, they can contact us to request a copy of their information. A contact form is available at https://www.facebook.com/help/contact/180237885820953.

10. At the House hearing, Congressman Welch asked if you believe that consumers should be able to correct or delete inaccurate personal data that companies have obtained about them. You did not answer that question completely.

a. Please state if you agree that consumers should be able to correct or delete information companies have collected about them. Explain your answer.

b. Please state if you agree that consumers should be able to correct or delete inferences companies have made about them based on information collected or otherwise obtained about them. Explain your answer.

Our Download Your Information or "DYI" tool is Facebook's data portability tool and was launched many years ago to let people access and download many types of information that we maintain about them. The data in DYI and in our Ads Preferences tool contain each of the interest categories that are used to show people ads, along with information about the advertisers that are currently running ads based on their use of an advertiser's website or app. People also can choose not to see ads from those advertisers. We recently announced expansions to Download Your Information, which, among other things, will make it easier for people to see their data, delete it, and easily download and export it. More information is available at https://newsroom.fb.com/news/2018/04/new-privacy-protections/.

Responding to feedback that we should do more to provide information about websites and apps that send us information when people use them, we also announced plans to build Clear History. This new feature will enable users to see the websites and apps that send us information when they use them, clear this information from their account, and turn off Facebook's ability to store it associated with their account going forward.

We have also introduced Access Your Information. This feature provides a new way for people to access and manage their information. Users can go here to delete anything from their timeline or profile that they no longer want on Facebook. They can also see their ad interests, as well as information about ads they've clicked on and advertisers who have provided us with information about them that influence the ads they see. From here, they can go to their ad settings to manage how this data is used to show them ads.

11. In response to a question from Congressman Tonko, you acknowledged that Facebook collects information from a person "visiting other places, then [users] have a way of getting access to that and deleting it and making sure that we don't store it anymore." Please explain in detail the way that users can get access to information collected from that user visiting other places and have that information deleted from Facebook's servers.

See Response to Question 10.

12. Congressman Tonko also asked whether Facebook bears liability when users' data is mishandled. Yes or no, is Facebook liable when Facebook users' data is mishandled? What recourse do Facebook users have?

Privacy is at the core of everything we do, and our approach to privacy starts with our commitment to transparency and control—to helping people understand how their data is collected and used, and to giving them meaningful controls. Our approach to control is based on the belief that people should be able to choose who can see what they share and how their data shapes their experience on Facebook and should have control over all data collection and uses that are not necessary to provide and secure our service. People can control the audience for their posts and the apps that can receive their data when they login with Facebook. They can control the people, Pages, Groups, and Events they connect to, and how they see content from those connections in their News Feeds. They can provide feedback on every post they see on Facebook—feedback, for example, that they want to see less of a particular kind of post or fewer posts from a particular person or Page. They can see and delete the history of their activities on Facebook, and, if they no longer want to use Facebook, they can delete their account and the data associated with it.

13. Congresswoman Clarke asked for a timeline of when the announced changes in how Facebook will review and verify the identity and location of advertisers running political or issue ads. You testified that those changes will be in place for these elections. Campaigns for these elections are already underway. Please clarify what you meant when you said the changes will be in place for these elections. Are those changes in place now?

All election-related and issue ads on Facebook and Instagram in the US must now be clearly labeled—including a "Paid for by" disclosure from the advertiser at the top of the ad. This will help ensure that people can see who is paying for the ad—which is especially important when the Page name doesn't match the name of the company or person funding the ad. When people click on the label, they'll be taken to an archive with more information. For example, the campaign budget associated with an individual ad and how many people saw it—including their age, location and gender. That same archive can be reached at https://www.facebook.com/politicalcontentads. People on Facebook visiting the archive can see and search ads with political or issue content an advertiser has run in the US for up to seven years. Advertisers wanting to run ads with political content in the US will need to verify their identity and location. Enforcement of these new features and the Political Ads policy, available at https://www.facebook.com/policies/ads/restricted_content/political, began on May 24.

14. In response to a question from Congressman Schrader, you testified that Facebook does "spot checks to make sure that the apps are actually doing what they say they are doing."

a. Please explain in detail the full process of a spot check.

b. How often do spot checks occur now?

c. When did Facebook begin doing these spot checks? How many spot checks have been done per month since Facebook first started doing spot checks of apps on its platform?

We use a variety of tools to enforce Facebook policies against violating parties, including developers. We review tens of thousands of apps per year and regularly disapprove noncompliant apps as part of our proactive review process. We also use tools like cease-and-desist letters, account suspensions, letter agreements, and civil litigation. For example, since 2006, Facebook has sent over 1,150 cease-and-desist letters to over 1,600 targets. In 2017, we took action against about 370,000 apps, ranging from imposing certain restrictions to removal of the app from the platform. Moreover, we have required parties who have procured our data without authorization to delete that data. We have invested significant resources in these efforts. Facebook is presently investigating apps that had access to large amounts of information before we changed our platform policies in 2014 to significantly reduce the data apps could access. As of early June 2018, around 200 apps (from a handful of developers: Kogan, AIQ, Cube You, the Cambridge Psychometrics Center, myPersonality, and AIQ) have been suspended—pending a thorough investigation into whether they did in fact misuse any data.

15. In response to a question from Congressman Kennedy, you testified that "the targeting options that are available for advertisers are generally things that are based on what people share."

a. When you said the options are "based on" what people share, does that include inferences made by Facebook or other parties and shared with Facebook?

b. What did you mean by "generally"? Please list all targeting options that are available for advertisers that are not based on what people share?

c. Please explain how Facebook makes or obtains inferences about people's interests. Are algorithms used to make those inferences? If so, please detail how those algorithms work. Use examples if necessary.

Facebook does not analyze the content of photos or text in users' posts or messages to target ads to them using AI or otherwise. Instead, there are a few primary ways that we personalize the ads and sponsored content for people on Facebook, based on:

- **Information from people's use of Facebook.** When people use Facebook, they can choose to share things about themselves like their age, gender, hometown, or interests. They can also click or like posts, Pages, or articles. We use this information to understand what users might be interested in and hopefully show them ads that are relevant. If a bike shop comes to Facebook wanting to reach female cyclists in Atlanta, we can show their ad to women in Atlanta who liked a Page about bikes. People can always see the "interests" assigned to them in their ad preferences, and if they want, remove them.

- **Information that an advertiser shares with us (or "custom audiences").** In this case, advertisers bring us the customer information so they can reach those people on Facebook. These advertisers might have people's email address from a purchase users made, or from some other data source. If we have matching email addresses, we can show those people ads from that advertiser (although we cannot see the email

addresses which are sent to us in hashed form, and these are deleted as soon as we complete the match). In ad preferences people can see which advertisers with their contact information are currently running campaigns—and they can click the top right corner of any ad to hide all ads from that business.

- **Information that websites and apps send to Facebook.** Some of the websites and apps people visit may use Facebook tools to make their content and ads more relevant, if people consent to let Facebook show them ads based on data from third-party partners. For example, if an online retailer is using Facebook Pixel, they can ask Facebook to show ads to people who looked at a certain style of shoe or put a pair of shoes into their shopping cart. If users don't want this data used to show them ads, they can turn it off in ad preferences.

- **Facebook also offers Lookalike Audiences.** Advertisers creating a Lookalike Audience choose a source audience (which could include a custom audience as described above, people who have opened or completed a form in lead ads on Facebook, people who have interacted with the advertiser's Facebook page or its Instagram profile). Facebook then identifies common qualities of the people in the source audience (e.g., demographic information or information about their interests), and then identifies people who are similar to them (on the basis of the common signals identified in the source audience), without sharing this information with the advertiser.

We have thousands of people whose job it is to help review ads for compliance with our policies. We recently announced that we are hiring thousands of additional reviewers this year.

16. You also noted a number of times at the hearings that Facebook announced that it was stopping working with data brokers as part of the ad system.

a. Yes or no, does Facebook currently acquire any information from data brokers under any circumstances or for any purpose? Will Facebook do so in the future?

b. If not for the ad system, for what purposes does or will Facebook acquire information from data brokers? Please detail all purposes for which Facebook uses data acquired from data brokers.

c. Facebook's data policy states that Facebook does acquire information about people from third-party partners. Please describe in detail what entities are considered third-party partners. Are any data brokers currently considered third- party partners?

d. Please describe in detail all categories of information Facebook obtains from third-party partners and all purposes for which the data are used.

e. Please detail how users can opt out of allowing Facebook to collect or store information about them acquired from third-party partners.

f. Facebook's data policy states that it shares Facebook users' information with certain third parties. Are any data brokers in the category of third parties with whom Facebook shares information?

g. It has been stated very clearly that Facebook does not sell information. Please describe the transactions between Facebook and these third parties. Is any form of non-monetary consideration, in-kind services, or other compensation transferred in exchange for the data? If so, please describe what was exchanged.

h. Please describe in detail all categories of information Facebook shares with third parties and all purposes for which the data are used.

i. Please detail how users can opt out of allowing Facebook to share information about them with third parties.

We believe that it's important to communicate with people about the information that we collect and how people can control it. That is why we work hard to provide this information to people in a variety of ways: in our Data Policy, and in Privacy Basics, which provides walkthroughs of the most common privacy questions we receive. Beyond simply disclosing our practices, we also think it's important to give people access to their own information, which we do through our Download Your Information and Access Your Information tools, Activity Log, and Ad Preferences, all of which are accessible through our Privacy Shortcuts tool. We also provide information about these topics as people are using the Facebook service itself.

We've heard loud and clear that privacy settings and other important tools are too hard to find and that we must do more to keep people informed. So, we're taking additional steps to put people more in control of their privacy. For instance, we redesigned our entire settings menu on mobile devices from top to bottom to make things easier to find. We also created a new Privacy Shortcuts in a menu where users can control their data in just a few taps, with clearer explanations of how our controls work. The experience is now clearer, more visual, and easy-to-find. Furthermore, we also updated our terms of service that include our commitments to everyone using Facebook. We explain the services we offer in language that's easier to read. We also updated our Data Policy to better spell out what data we collect and how we use it in Facebook, Instagram, Messenger, and other products.

Depending on which Services a person uses, we collect different kinds of information from or about them. This is described in our Data Policy:

- **Things users and others do and provide**. Information and content users provide. We collect the content, communications and other information users provide when they use our Products, including when they sign up for an account, create or share content, and message or communicate with others. This can include information in or about the content they provide (like metadata), such as the location of a photo or the date a file was created. It can also include what users see through features we provide, such as our camera, so we can do things like suggest masks and filters that they might like, or give users tips on using camera formats. Our systems automatically process content and

communications users provide to analyze context and what's in them for the purposes described below. People can learn more about how they can control who can see the things they share here: https://www.facebook.com/help/1297502253597210?ref=dp.

    - Data with special protections: Users can choose to provide information in their Facebook profile fields or Life Events about their religious views, political views, who they are "interested in," or their health. This and other information (such as racial or ethnic origin, philosophical beliefs, or trade union membership) could be subject to special protections under the laws of their country.

- **Networks and connections.** We collect information about the people, Pages, accounts, hashtags, and groups users are connected to and how they interact with them across our Products, such as people a user communicates with the most or groups users are part of. We also collect contact information if they choose to upload, sync, or import it from a device (such as an address book or call log or SMS log history), which we use for things like helping them and others find people they may know and for the other purposes listed in our Data Policy.

- **People's usage.** We collect information about how people use our Products, such as the types of content they view or engage with; the features they use; the actions they take; the people or accounts they interact with; and the time, frequency, and duration of their activities. For example, we log when they're using and have last used our Products, and what posts, videos, and other content they view on our Products. We also collect information about how they use features like our camera.

- **Information about transactions made on our Products.** If people use our Products for purchases or other financial transactions (such as when users make a purchase in a game or make a donation), we collect information about the purchase or transaction. This includes payment information, such as their credit or debit card number and other card information; other account and authentication information; and billing, shipping, and contact details.

- **Things others do and information they provide about users**. We also receive and analyze content, communications, and information that other people provide when they use our Products. This can include information about them, such as when others share or comment on a photo of a user, send a message to them, or upload, sync or import their contact information.

- **Device Information**. As described below, we collect information from and about the computers, phones, connected TVs and other web-connected devices they use that integrate with our Products, and we combine this information across different devices they use. For example, we use information collected about their use of our Products on their phone to better personalize the content (including ads) or features they see when they use our Products on another device, such as their laptop or tablet, or to measure whether they took an action in response to an ad we showed them on their phone on a different device.

- Information we obtain from these devices includes:
    - Device attributes: information such as the operating system, hardware and software versions, battery level, signal strength, available storage space, browser type, app and file names and types, and plugins.
    - Device operations: information about operations and behaviors performed on the device, such as whether a window is foregrounded or backgrounded, or mouse movements (which can help distinguish humans from bots).
    - Identifiers: unique identifiers, device IDs, and other identifiers, such as from games, apps or accounts people use, and Family Device IDs (or other identifiers unique to Facebook Company Products associated with the same device or account).
    - Device signals: Bluetooth signals, and information about nearby Wi-Fi access points, beacons, and cell towers.
    - Data from device settings: information users allow us to receive through device settings people turn on, such as access to their GPS location, camera, or photos.
    - Network and connections: information such as the name of users' mobile operator or ISP, language, time zone, mobile phone number, IP address, connection speed and, in some cases, information about other devices that are nearby or on users' network, so we can do things like help people stream a video.
    - Cookie data: data from cookies stored on a user's device, including cookie IDs and settings. Learn more about how we use cookies in the Facebook Cookies Policy (https://www.facebook.com/policies/cookies/) and Instagram Cookies Policy (https://www.instagram.com/legal/cookies/).

- **Information from partners**. Advertisers, app developers, and publishers can send us information through Facebook Business Tools they use, including our social plug-ins (such as the Like button), Facebook Login, our APIs and SDKs, or the Facebook pixel. These partners provide information about users' activities off Facebook—including information about a user's device, websites users visit, purchases users make, the ads they see, and how they use their services—whether or not they have a Facebook account or are logged into Facebook. For example, a game developer could use our API to tell us what games users play, or a business could tell us about a purchase a user made in its store. We also receive information about a user's online and offline actions and purchases from third-party data providers who have the rights to provide us with their information. Partners receive user data when users visit or use their services or through third parties

they work with. We require each of these partners to have lawful rights to collect, use and share user data before providing any data to us.

People own what they share on Facebook, and they can manage things like who sees their posts and the information they choose to include on their profile. More information about how we share information is available in our Data Policy (https://www.facebook.com/about/privacy).

Our Download Your Information or "DYI" tool is Facebook's data portability tool and was launched many years ago to let people access and download many types of information that we maintain about them. The data in DYI and in our Ads Preferences tool contain each of the interest categories that are used to show people ads, along with information about the advertisers that are currently running ads based on their use of an advertiser's website or app. People also can choose not to see ads from those advertisers. We recently announced expansions to Download Your Information, which, among other things, will make it easier for people to see their data, delete it, and easily download and export it. More information is available at https://newsroom.fb.com/news/2018/04/new-privacy-protections/.

And we recently announced plans to build Clear History. This feature will enable users to see the websites and apps that send us information when they use them, clear this information from their accounts, and turn off our ability to store it associated with their accounts going forward. It will take a few months to build Clear History. We'll work with privacy advocates, academics, policymakers, and regulators to get their input on our approach, including how we plan to remove identifying information and the rare cases where we need information for security purposes. We've already started a series of roundtables in cities around the world and heard specific demands for controls like these at a session we held at our headquarters. We're looking forward to doing more.

Apps and websites that use features such as the Like button or Facebook Analytics send us information to make their content and ads better. We also use this information to make users' experiences on Facebook better. If a user clears their history or uses the new setting, we'll remove identifying information so a history of the websites and apps they've used won't be associated with their account. We'll still provide apps and websites with aggregated analytics—for example, we can build reports when we're sent this information so we can tell developers if their apps are more popular with men or women in a certain age group. We can do this without storing the information in a way that's associated with a user's account, and as always, we don't tell advertisers who a user is.

We have also introduced Access Your Information. This feature provides a new way for people to access and manage their information. Users can go here to delete anything from their timeline or profile that they no longer want on Facebook. They can also see their ad interests, as well as information about ads they've clicked on and advertisers who have provided us with information about them that influence the ads they see. From here, they can go to their ad settings to manage how this data is used to show them ads.

17. Congresswoman Dingell asked some questions to which you did not have responses. Please provide responses to the following for the record.

a. How many Facebook Like buttons are there on non-Facebook web pages?

b. How many Facebook Share buttons are there on non-Facebook web pages?

c. How many Facebook Pixels are there on non-Facebook web pages?

During the week prior to April 16, 2018, on sites that use Facebook services, the Like button appeared on 8.4 million websites, the Share button on 931,000 websites covering 275 million webpages, and there were 2.2 million Facebook pixels installed on websites.

18. When a Facebook user uploads his or her contact list or address book so that Facebook can suggest people they may know and want to connect to on the platform, Facebook collects and stores the names and contact information of all of those people in the user's contact list, whether or not those people are Facebook users themselves.

a. Please identify the website or pop-up or any place where Facebook users have consented to allow Facebook to collect and store their contact information uploaded by another user.

b. Please identify the website or pop-up or any place where those people who have never signed up for a Facebook account have consented to allow Facebook to collect and store their contact information uploaded by a Facebook user.

c. We know Facebook uses contact information to suggest people users can connect to. Please describe in detail all other ways and reasons Facebook uses contact information of people that never voluntarily shared their own contact information with Facebook.

Call and text history logging is part of an opt-in feature that lets people import contact information to help them connect with people they know on Facebook and Messenger. We introduced the call and text history component of this feature for Android users several years ago, and currently offer it in Messenger and Facebook Lite, a lightweight version of Facebook, on Android.

Contact importers are fairly common among social apps and serve as a way to more easily find the people users want to connect with. They help users find and stay connected with the people they care about and provide them with a better experience across Facebook.

Before we receive call and text history from people, they specifically grant us permission to access this data on their device and separately agree to use the feature. If, at any time, they no longer wish to use this feature they can turn it off, and all previously shared call and text history shared via that app is deleted. People can also access information they previously imported through the Download Your Information tool.

We've reviewed this feature to confirm that Facebook does not collect the content of messages—and will delete all logs older than one year. In the future, people will only upload to our servers the information needed to offer this feature—not broader data such as the time of calls. We do allow people from 13 to 17 to opt into this service. However, we do take other steps to protect teens on Facebook and Messenger:

- We provide education before allowing teens to post publicly.
- We don't show search results based on specific profile data (high school, birthday/age, and hometown, or current city) of teens to unconnected adults when the adults search on Facebook.
- Unconnected adults can't message minors who are 13-17.
- We have age limits for advertisements. For example, ads for dating sites, financial services and other products or services are gated to users under 18. We've also helped many teenagers with information about bullying prevention campaigns and online safety tips, including creating a new website full of privacy and safety resources for teens: https://www.facebook.com/safety/youth.
- Contact importers are common on mobile devices and many web and mobile social apps and, on Facebook, serve as a way to more easily find the people users want to connect or communicate with (without having to type in all of the individual entries that a user may maintain in their device address book, to be able to use that information again on Facebook, Instagram or Messenger). They help users find and stay connected with the people they care about and provide them with a better experience across Facebook.
- The Android and iOS operating systems enable apps to ask users for permission to access contact list information as part of their standard documented APIs.
- We obtain express consent in our products from people before they can upload their contacts to Facebook, and we further disclose this practice in our Data Policy and recently updated the language to provide additional transparency. The Data Policy states:
    - Networks and connections. We collect information about the people, Pages, accounts, hashtags, and groups users are connected to and how they interact with them across our Products, such as people a user communicates with the most or groups users are part of. We also collect contact information if they choose to upload, sync, or import it from a device (such as an address book or call log or SMS log history), which we use for things like helping them and others find people they may know and for the other purposes listed in our Data Policy.

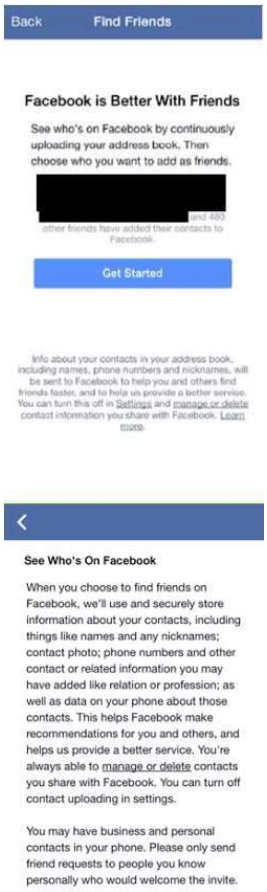
Further, when people create Facebooks accounts people are offered the opportunity to upload their contact list, which helps them connect with friends and improve people's Facebook

experience. This prompt provides details on how we use the information (see below). Further, when people create Facebooks accounts people are offered the opportunity to upload their contact list, which helps them connect with friends and improve people's Facebook experience. This prompt provides details on how we use the information (see below).

We disclose how we use contacts in our Data Policy. We let people upload all of the contacts in their address book on their device, whether or not those contacts involve registered users or not (since the user choosing to upload ultimately controls what goes into their address book and is choosing to take that information to various services to use it). The uploader can access or remove these contacts at anytime as described here: https://www.facebook.com/help/355489824655936.

When joining Facebook, a person must provide basic contact information (like an email address or a phone number) in order to register for an account. This helps us communicate with them, ensure account security and helps ensure that when people want to receive friend requests or other communications outside of the app, those communications get to the right person.

When a person uploads contact information that we're unable to match to a Facebook account, we make it possible for the user to invite their contact to join Facebook or to attend events. When someone new to Facebook signs up for an account, we also use the fact that their contact information was uploaded to Facebook to suggest people they might want to be friends with, as well as determine whether the new account is genuine and not fake.



19. Facebook's data policy states that Facebook tracks location through GPS, Bluetooth, and WiFi signals and that such information is used to "tailor our Services for you and others."

a. Please explain in detail how location data is used to tailor services for users. Also explain in detail all the ways and purposes for which Facebook uses location information.

As our Data Policy indicates, "When we have location information, we use it to tailor our Services for you and others, like helping you to check-in and find local events or offers in your area or tell your friends that you are nearby."

We use data from devices (such as location data) to help advertisers reach people in particular areas. For example, if people have shared their device locations with Facebook or checked into a specific restaurant, we can show them ads from an advertiser that wants to promote its services in their area or from the restaurant.

b. Please detail how users can opt out of allowing Facebook to collect or store location information.

All users must expressly consent to Facebook's Terms and Data Policy when registering for Facebook. The Data Policy explains the kinds of information we collect, how we use this information, how we share this information, and how you can manage and delete information. After joining Facebook, people are presented with the opportunity to consent to additional data collection and uses, such as the Location Services permission on Android and iOS devices, which they can grant or revoke at any time.

c. Please detail how users can delete location information stored on Facebook's servers.

We enable people, including people in the United States, to learn more about the data we collect through interactive tools such as Download Your Information, which lets people download a file containing data that they may want to take to another service, and through Access Your Information, a tool we've launched for people to more easily access and manage their data on Facebook. People can also control their information through their Settings and the Privacy Shortcuts tool that we're rolling out now.

20. Facebook reportedly tracks whether a window open on a person's computer is in the foreground or background and the movements of a person's mouse.

a. Please describe all the ways that such data is used by Facebook.

b. Please identify the website or pop-up or any place where Facebook users have consented to allow Facebook to collect and store such data.

c. Please detail how users can opt out of allowing Facebook to collect or store such data.

Facebook's services inherently operate on a cross-device basis: understanding when people use our services across multiple devices helps us provide the same personalized experience wherever people use Facebook—for example, to ensure that a person's News Feed or profile contains the same content whether they access our services on their mobile phone or in a desktop computer's web browser.

In support of those and other purposes, we collect information from and about the computers, phones, connected TVs and other web-connected devices our users use that integrate with our Products, and we combine this information across a user's different devices. For example, we use information collected about a person's use of our Products on their phone to better personalize the content (including ads) or features they see when they use our Products on another device, such as their laptop or tablet, or to measure whether they took an action in response to an ad we showed them on their phone or on a different device.

Information we obtain from these devices includes:

- **Device attributes.** Information such as the operating system, hardware and software versions, battery level, signal strength, available storage space, browser type, app and file names and types, and plugins.

- **Device operations.** Information about operations and behaviors performed on the device, such as whether a window is foregrounded or backgrounded, or mouse movements (which can help distinguish humans from bots).

- **Identifiers.** Unique identifiers, device IDs, and other identifiers, such as from games, apps or accounts people use, and Family Device IDs (or other identifiers unique to Facebook Company Products associated with the same device or account).

- **Device signals.** Bluetooth signals, and information about nearby Wi-Fi access points, beacons, and cell towers.

- **Data from device settings.** Information a user allows us to receive through device settings they turn on, such as access to their GPS location, camera, or photos.

- **Network and connections.** Information such as the name of a user's mobile operator or ISP, language, time zone, mobile phone number, IP address, connection speed and, in some cases, information about other devices that are nearby or on their network, so we can do things like help them stream a video from their phone to their TV.

- **Cookie data.** Data from cookies stored on a user's device, including cookie IDs and settings. More information is available at https://www.facebook.com/policies/cookies/ and https://help.instagram.com/1896641480634370?ref=ig.

Advertisers, app developers, and publishers can send us information through Facebook Business Tools they use, including our social plug-ins (such as the Like button), Facebook Login, our APIs and SDKs, or the Facebook pixel. These partners provide information about a person's activities off Facebook—including information about their device, websites they visit, purchases they make, the ads they see, and how they use their services—whether or not they have a Facebook account or are logged into Facebook. For example, a game developer could use our API to tell us what games a person plays, or a business could tell us about a purchase a person made in its store. We also receive information about a person's online and offline actions and purchases from third-party data providers who have the rights to provide us with that person's information.

We use the information we have to deliver our Products, including to personalize features and content (including a person's News Feed, Instagram Feed, Instagram Stories, and ads) and make suggestions for a user (such as groups or events they may be interested in or topics they may want to follow) on and off our Products. To create personalized Products that are unique and relevant to them, we use their connections, preferences, interests, and activities based on the data we collect and learn from them and others (including any data with special protections they

choose to provide); how they use and interact with our Products; and the people, places, or things they're connected to and interested in on and off our Products.

For example, if people have shared their device locations with Facebook or checked into a specific restaurant, we can show them ads from an advertiser that wants to promote its services in their area or from the restaurant. We use location-related information—such as a person's current location, where they live, the places they like to go, and the businesses and people they're near—to provide, personalize and improve our Products, including ads, for them and others. Location-related information can be based on things like precise device location (if a user has allowed us to collect it), IP addresses, and information from their and others' use of Facebook Products (such as check-ins or events they attend). We store data until it is no longer necessary to provide our services and Facebook Products, or until a person's account is deleted—whichever comes first. This is a case-by-case determination that depends on things like the nature of the data, why it is collected and processed, and relevant legal or operational retention needs. We provide advertisers with reports about the kinds of people seeing their ads and how their ads are performing, but we don't share information that personally identifies someone (information such as a person's name or email address that by itself can be used to contact them or identifies who they are) unless they give us permission. For example, we provide general demographic and interest information to advertisers (for example, that an ad was seen by a woman between the ages of 25 and 34 who lives in Madrid and likes software engineering) to help them better understand their audience. We also confirm which Facebook ads led people to make a purchase or take an action with an advertiser.

21. Facebook collects and stores information about users that has been shared by other users.

a. Please explain how users can see what information Facebook has stored about them that was collected from other users and how it is identified as information collected from other users.

b. Please detail how users can opt out of allowing Facebook to collect or store information about them collected from other users.

c. Please detail how users can delete information about them collected from other users stored on Facebook's servers.

People join Facebook in order to connect to the people, content, and businesses that are most meaningful to them. We use information we collect from users and their friends and contacts in order to create a personalized experience that is unique to each person and to enable them to make better connections—such as tagging friends in a post or a photo or uploading contacts to help find people they know on Facebook. Our Data Policy clearly explains this to users and is available at https://www.facebook.com/privacy/explanation.

We know people sometimes might not like the information others have shared, so we provide a number of tools to notify and help people resolve concerns. For example, if another person makes a post about someone, we provide tools to notify the person if they were tagged in that post as explained here: https://www.facebook.com/help/124970597582337/. Similarly, if a

person has enabled face recognition, we provide notifications to them when people post a picture of them, as explained here: https://www.facebook.com/help/135566640422874. We also provide social resolution tools to help people ask others to take down content about them, as explained here: https://www.facebook.com/help/128548343894719. We store uploaded contacts relating people on behalf of the person who uploaded them. The uploader can access or remove these contacts at anytime as described here: https://www.facebook.com/help/355489824655936We. Finally, our community standards prohibit the posting of personal or confidential information of others without consent, as explained here: https://www.facebook.com/communitystandards/safety/privacy_violations_image_rights/. We will take down content that violates this policy.

Our Download Your Information or "DYI" tool is Facebook's data portability tool and was launched many years ago to let people access and download many types of information that we maintain about them. The data in DYI and in our Ads Preferences tool contain each of the interest categories that are used to show people ads, along with information about the advertisers that are currently running ads based on their use of an advertiser's website or app. People also can choose not to see ads from those advertisers. We recently announced expansions to Download Your Information, which, among other things, will make it easier for people to see their data, delete it, and easily download and export it. More information is available at https://newsroom.fb.com/news/2018/04/new-privacy-protections/.

We have also introduced Access Your Information. This feature provides a new way for people to access and manage their information. Users can go here to delete anything from their timeline or profile that they no longer want on Facebook. They can also see their ad interests, as well as information about ads they've clicked on and advertisers who have provided us with information about them that influence the ads they see. From here, they can go to their ad settings to manage how this data is used to show them ads.

22. At the House hearing, Congressman Lujan mentioned that in 2013, Brandon Copley, the CEO of Giftnix, demonstrated that a search feature on Facebook could easily be used to scrape information at scale. He also stated that the issue of data scraping was raised again by a security researcher in 2015. Only this year did Facebook disable that search feature. Facebook knew since at least 2013 that this search could be exploited. Why did it take so long for Facebook to take action? What made Facebook decide in April 2018 to finally disable that feature?

In April, we found out that a feature that lets users look someone up by their phone number and email may have been misused by browsers looking up people's profiles in large volumes with phone numbers they already had. When we found out about the abuse, we shut this feature down. In the past, we have been aware of scraping as an industry issue, and have dealt with specific bad actors previously.

23. At the House hearing, you were asked a number of times to clarify whether Facebook would be providing the same protections and rights to Americans that will be given to citizens of the European Union under the General Data Protection Regulation (GDPR). You stated multiple times that the same "controls" will be

available to all Facebook users across the world. But I think your answer was very careful. Controls are not the same as rights and protections.

a. Congressman Green asked you about the provision in the GDPR that gives users the right to object to the processing of their personal data for marketing purposes. You did not have an answer at the hearing, so please answer now. Will the same rights be available to Facebook users in the United States? When and how will that be implemented?

b. Congressman Green also asked about the data portability requirement under GDPR. Please explain in detail how and when that requirement will be implemented for Facebook users in the United States.

c. Following the hearing, news outlets reported that Facebook is intending to change its terms of service to put all non-European users under the jurisdiction of Facebook's U.S. headquarters. This move reportedly would make it so that all non-European users would not be subject to the rights and protections afforded people under the GDPR and Facebook would not be subject to enforcement and fines under GDPR with respect to non-European users. If Facebook is granting the same protections to everyone, why is Facebook making this change?

d. Please explain in detail the differences between the rights, protections, and controls that Facebook is guaranteeing to European citizens under the GDPR and the rights, protections, and controls that Facebook will provide to non-European citizens in relation the GDPR.

As a part of our overall approach to privacy, we are providing the same tools for access, rectification, erasure, data portability and others to people in the US (and globally) that we provide in the European Union under the GDPR. The controls and settings that Facebook is enabling as part of GDPR include settings for controlling our use of face recognition on Facebook and for controlling our ability to use data we collect off Facebook Company Products to target ads. We recently began providing direct notice of these controls and our updated terms to people around the world (including in the US), allowing people to choose whether or not to enable or disable these settings or to consent to our updated terms. Many of these tools (like our Download Your Information tool, which is Facebook's data portability tool; ad preferences tool; and Activity Log) have been available globally for many years.

The substantive protections in our user agreements offered by Facebook Ireland and Facebook, Inc. are the same. However, there are certain aspects of our Facebook Ireland Data Policy that are specific to legal requirements in the GDPR—such as the requirement that we provide contact information for our EU Data Protection Officer or that we identify the "legal bases" we use for processing data under the GDPR. Likewise, our Facebook Ireland terms and Data Policy address the lawful basis for transferring data outside the EU, based on legal instruments that are applicable only to the EU. And other provisions of the GDPR itself pertain to interactions between European regulators and other matters that are not relevant to people located outside of the EU.

We are seeking explicit consent from people in Europe to three specific uses of data: facial recognition data (which previously was not enabled in Europe), special categories of data, and use of data we collect off Facebook Company Products to target ads. As noted above, we recently began providing direct notice of these controls and our updated terms to people around the world (including in the US), allowing people to choose whether or not to enable or disable these settings or to agree to our updated terms. Outside of Europe we are not requiring people to complete those flows if they repeatedly indicate that they do not want to go through the experience. At the same time, the events of recent months have underscored how important it is to make sure people know how their information is used and what their choices are. So, we decided to communicate prominently on Facebook—through a full-screen message and a reminder to review at a later date. People can choose to dismiss or ignore these messages and continue using Facebook.

The Honorable Bobby L. Rush

1. On April 4, 2018, I sent you a letter to learn more about how Facebook will implement the global rollout of the European Union's General Data Protection Regulation (GDPR). Even now, it remains unclear on how Facebook will implement these protections for users in the United States. Specifically:

a. What specific provisions of the GDPR will be implemented in the United States and how?

As a part of our overall approach to privacy, we are providing the same tools for access, rectification, erasure, data portability and others to people in the US (and globally) that we provide in the European Union under the GDPR. The controls and settings that Facebook is enabling as part of GDPR include settings for controlling our use of face recognition on Facebook and for controlling our ability to use data we collect off Facebook Company Products to target ads. We recently began providing direct notice of these controls and our updated terms to people around the world (including in the US), allowing people to choose whether or not to enable or disable these settings or to consent to our updated terms. Many of these tools (like our Download Your Information tool, which is Facebook's data portability tool; ad preferences tool; and Activity Log) have been available globally for many years.

The substantive protections in our user agreements offered by Facebook Ireland and Facebook, Inc. are the same. However, there are certain aspects of our Facebook Ireland Data Policy that are specific to legal requirements in the GDPR—such as the requirement that we provide contact information for our EU Data Protection Officer or that we identify the "legal bases" we use for processing data under the GDPR. Likewise, our Facebook Ireland terms and Data Policy address the lawful basis for transferring data outside the EU, based on legal instruments that are applicable only to the EU. And other provisions of the GDPR itself pertain to interactions between European regulators and other matters that are not relevant to people located outside of the EU.

Facebook is subject to ongoing oversight by the Federal Trade Commission with respect to its privacy commitments to people and its implementation of privacy settings, under a Consent Order with the FTC. Facebook is subject to the authority of the Irish Data Protection Commissioner, its lead regulator, under the GDPR in the European Union.

b. How will users be able to verify that certain rights (e.g., the Right to be Forgotten) are being upheld?

See Response to Question 1(a).

c. In your testimony, you mentioned several times that Facebook collects data of nonusers for "security purposes." How can these individuals, who do not have a Facebook account, ensure their information is deleted and how they can opt-out of Facebook's data collection?

If a person doesn't have a Facebook account but believes Facebook may have information about them, they can contact us to request a copy of their information. A contact form is available at https://www.facebook.com/help/contact/180237885820953.

d. Will GDPR protections be the default setting or will users have to manually opt-in to them? If they will not be the default settings, why not?

We are seeking explicit consent from people in Europe to three specific uses of data: facial recognition data (which previously was not enabled in Europe), special categories of data, and use of data we collect off Facebook Company Products to target ads. We recently began providing direct notice of these controls and our updated terms to people around the world (including in the US), allowing people to choose whether or not to enable or disable these settings or to agree to our updated terms. Outside of Europe we are not requiring people to complete those flows if they repeatedly indicate that they do not want to go through the experience. At the same time, the events of recent months have underscored how important it is to make sure people know how their information is used and what their choices are. So, we decided to communicate prominently on Facebook—through a full-screen message and a reminder to review at a later date. People can choose to dismiss or ignore these messages and continue using Facebook.

GDPR does not require consent for most uses of personal information, and instead, recognizes that many uses of data are necessary to provide a service or within companies' legitimate interests or the public interest. We agree that different levels of consent or notice are appropriate depending on the type of information or contemplated use at issue.

e. What is the anticipated timeline for implementing provisions of the GDPR in the United States?

See Response to Question 1(a).

2. This matter is being discussed in Congress and around the world because a whistleblower came forward and revealed what was happening. If not for this individual's actions, how much longer would Facebook users have had to wait before they were notified that their data had been misused? Would Facebook be announcing and rolling out updates to its privacy policy and business practices that are not mandated by the EU's GDPR? If no, why not? Would Facebook be making the GDPR's protections available worldwide? If no, why not?

When Facebook learned about Kogan's breach of Facebook's data use policies in December 2015, we took immediate action. Facebook immediately banned Kogan's app from our developer platform. We retained an outside firm to assist in investigating Kogan's actions, to demand that Kogan and each party he had shared data with delete the data and any derivatives of the data, and to obtain certifications that they had done so. Because Kogan's app could no longer collect most categories of data due to changes in Facebook's platform, the company's highest priority at that time was ensuring deletion of the data that Kogan may have accessed before these changes took place. With the benefit of hindsight, we wish we had notified people whose

information may have been impacted. Facebook has since notified all people potentially impacted with a detailed notice at the top of their News Feed.

Although our developer terms gave us the ability to audit Kogan's app, we did not have an agreement in place that would have allowed us to audit third parties that he may have shared data with. For this reason, we chose to require him to obtain certifications of deletion from each of these parties, leveraging our rights as to Kogan, who was the developer of the app.

In March 2018, Facebook received information from the media that possible questions existed around the validity of deletion certifications that Facebook received. In response, Facebook immediately banned Cambridge Analytica and other potentially related parties from distributing advertising on Facebook or from using other aspects of our service. At that time, we requested an on-site audit of Cambridge Analytica, which it agreed to. The forensic auditor's work is currently on hold at the request of UK regulatory authorities, who themselves are investigating Cambridge Analytica, which is located in the UK, and we are actively cooperating with the UK authorities to progress this analysis.

It is important to clarify that Kogan's improper disclosure of Facebook data that users shared with him does not involve a data breach on Facebook's platform. There was no unauthorized access to Facebook data by Kogan, and instead, his app could only access Facebook data that users specifically consented to share with him. Even though Kogan's improper disclosure of data was not a breach of our systems, these actions violate our Platform policy—and we took extensive measures to try to mitigate any potential misuse of that data by downstream parties by pushing aggressively for deletion. And we are implementing an approach that goes beyond legal requirements and informs people any time we learn that an app developer shared data with a third-party in violation of our policies. This is consistent with the responsibility we believe we have with our users, even if the law does not require this.

On your question about the GDPR, see Response to Question 1(a). We not only want to comply with the law, but also go beyond our obligations to build new and improved privacy experiences for everyone on Facebook.

3. You have said in the press that you support regulation and strong data and privacy protections. Since this latest release of data occurred while Facebook is operating under a consent decree from the Federal Trade Commission (FTC), it is clear that additional statutory authority is needed. My bill, H.R. 5388, mandates that the FTC issue regulations regarding a national framework for data privacy and data protection, specifies a timeline for notification, and clarifies what qualifies as personal information. Do you support enacting such protections in the United States? If no, why not?

Facebook is generally not opposed to regulation but wants to ensure it is the right regulation. We are already regulated in many ways—for example, under the Federal Trade Commission Act—and we are subject to ongoing oversight by the FTC under the terms of a 2011 Consent Order. Facebook has inherent incentives to protect its customers' privacy and address breaches and vulnerabilities. Indeed, the recent discovery of misconduct by an app developer on the Facebook platform clearly hurt Facebook and made it harder for us to achieve our social

mission. As such, Facebook is committed to protecting our platform from bad actors, ensuring we are able to continue our mission of giving people a voice and bringing them closer together. We are also actively building new technologies to help prevent abuse on our platform, including advanced AI tools to monitor and remove fake accounts. We have also significantly increased our investment in security, employing more than 15,000 individuals working solely on security and content review and planning to increase that number to over 20,000 by the end of the year. We have also strengthened our advertising policies, seeking to prevent discrimination while improving transparency.

4. What, specifically, is Facebook doing to ensure that advertisers do not wrongly exclude individuals from housing, employment, credit, and public accommodation ads based on gender, ethnic affinity, age, veteran status, disability, or other protected characteristics? In your testimony you stated that Facebook has "removed the option for advertisers to exclude ethnic groups from targeting." As we all know, indicating an interest or affinity for certain pages/groups/etc. would also allow advertisers to, rightly or wrongly, discern an individual's identity and if they are a member of a protected class. Does Facebook allow advertisers to target or exclude users based off their protected characteristics? If so, when will Facebook commit to removing this option?

We have Community Standards that prohibit hate speech, bullying, intimidation, and other kinds of harmful behavior. We hold advertisers to even stricter advertising policies to protect users from things like discriminatory ads. We don't want advertising to be used for hate or discrimination, and our policies reflect that. For example, our Advertising Policies make it clear that advertisers may not discriminate against people based on personal attributes such as race, ethnicity, color, national origin, religion, age, sex, sexual orientation, gender identity, family status, disability, and medical or genetic condition. The Policies also prohibit asserting or implying that a person belongs to one of these groups.

We educate advertisers on our anti-discrimination policy, and when we detect that an advertiser is attempting to run a housing, employment or credit ad, we require the advertiser to certify compliance with our anti-discrimination policy and anti-discrimination laws. We are committed to getting better at enforcing our advertising policies. We review many ads proactively using automated and manual tools, and reactively when people hide, block, or mark ads as offensive. We are taking aggressive steps to strengthen both our automated and our manual review. We are also expanding our global ads review teams and investing more in machine learning to better understand when to flag and take down ads, such as ads that use our multicultural affinity segments in connection with offers of housing, employment or credit opportunities.

5. Facebook and its many subsidiaries provide various forms of communication including, in one form or another, telephone and videoconferencing services; services often seen in the traditional telecommunication field. NASDAQ has even classified Facebook under the "Communication Services" umbrella. Do you believe that Facebook's offering of these services should be subject to Federal Communications Commission jurisdiction, specifically Title II privacy regulations? If no, why not?

The Federal Communications Commission (FCC) has long held the authority to protect the privacy of customers of telecommunication services. These privacy rules, pursuant to section 222 of the Communications Act and accompanying regulations, have applied to traditional telephony. Although certain of Facebook's services are somewhat analogous to traditional telephone calls, Facebook's services are meaningfully distinct—both technologically and legally. Facebook's services are presently limited to registered users, so that, for example, a Messenger user can only communicate with another Messenger user. By contrast, the FCC has applied its privacy rules only to interconnected services that rely on the public switched telephone network, i.e., where calls can be received from or terminated to any other phone number. Consequently, Facebook's communications functionality does not fall within the FCC's privacy rules.

6. In 2017, the world bore witness to the worst of humanity when, in Chicago, Facebook was used to disseminate violent videos of gangrape and an assault on the disabled through the Facebook Live feature. Though Facebook did ultimately remove the videos, this was not until after the broadcast had ended. Beyond removing them, what was done to ensure that similarly violent, disturbing, and illegal activities are not promoted and disseminated through your platform? What safeguards are in place to prevent materials that violate your community standards from reaching children? How does Facebook protect legitimate journalistic interest while limiting the spread of violent and extremist propaganda? Why has Facebook resisted implementing algorithm-based technologies — that have proven effective against child pornography— to stop the spread of violent content?

We're deeply saddened when the tools we've developed to help people come together and share experiences with their friends and family are misused. When someone does violate our Community Standards while using Live, we are committed to interrupting these streams as quickly as possible and we've provided people a way to report violations during a live broadcast. We will also notify law enforcement if we see a threat that requires an immediate response, and suggest people contact emergency services themselves if they become aware of a situation where the authorities can help.

For example, we are using machine learning to better detect and action on content and people that should not be using our platform. We recently shared how we are using machine learning to prevent bad actors like terrorists or scammers from using our platform (https://www.facebook.com/notes/facebook-security/introducing-new-machine-learning-techniques-to-help-stop-scams/10155213964780766/).

Of course, we cannot rely on technology alone to keep our community safe. A photo of an armed man waving an ISIS flag might be propaganda or recruiting material, but could be an image in a news story. To understand context and more nuanced cases, we need human expertise.

We are doubling the size of our security and content review teams (from 10,000 to 20,000) over the course of this year. We currently have approximately 15,000 people working on these teams. Of that 15,000, more than 7,500 people review content around the world.

- Our content review team is global and reviews reports in over 50 languages.

- Reports are reviewed 24 hours a day, 7 days a week and the vast majority of reports are reviewed within 24 hours.

- Our goal is always to have the right number of skilled people with the right language capabilities to ensure incoming reports are reviewed quickly and efficiently.

- We hire people with native language and other specialist skills according to the needs we see from incoming reports.

- The team also includes specialists in areas like child safety, hate speech and counter-terrorism, software engineers to develop review systems, quality control managers, policy specialists, legal specialists, and general reviewers.

We employ a mix of full-time employees, contractors, and vendor partners to assist with content review and help us scale globally. We partner with reputable vendors who are required to comply with specific obligations, including provisions for resiliency, support, transparency, and user privacy.

7. Multiple reports have suggested that Facebook has played a role in the persecution and genocide of the Rohingya fleeing Burma. Marzuki Darusman, the chairman of the UN Independent International Fact-Finding Mission on Myanmar, has gone as far as to say that Facebook played a "determining role". In your Vox interview, you said that Facebook systems detected the hate speech and allowed Facebook to stop it; an assertion that Burmese civic groups allege is false. According to them, the groups themselves were the "systems" that alerted Facebook that there was a problem and, by their own admission, their alerts were not comprehensive. What is Facebook doing to systematically detect and stop hate speech, violence, and extremism from spreading on your platform? How will Facebook do this without stifling legitimate activism and organizing?

We've been too slow to deal with the hate and violence in places like Myanmar and Sri Lanka. The challenges we face in a country that has fast come online are very different than those in other parts of the world, and we are investing in people, technology, and programs to help address them as effectively as possible.

Our content review teams around the world—which grew by 3,000 people last year—work 24 hours a day and in over 50 languages. Over the last two years, we have added dozens more Burmese language reviewers to handle reports from users across our services, and we plan to more than double the number of content reviewers focused on user reports. We also have increased the number of people across the company working on Myanmar-related issues and we have a special product team working to better understand the local challenges and build the right tools to help keep people in the country safe. We will continue to hire more staff dedicated to Myanmar, including Burmese speakers and policy experts. In Sri Lanka, we are increasing the number of Sinhalese language experts sevenfold.

That said, there is more to tackling this problem than reported content. A lot of abuse may go unreported, which is why we are supplementing our hiring with investments in

technology and programs. We are building new tools so that we can more quickly and effectively detect abusive, hateful, or false content. We have, for example, designated several hate figures and organizations for repeatedly violating our hate speech policies, which has led to the removal of accounts and content that support, praise, or represent these individuals or organizations. We are also investing in artificial intelligence that will help us improve our understanding of dangerous content.

From a programmatic perspective, we will continue to work with experts to develop safety resources and counter-speech campaigns in these regions and conduct regular training for civil society and community groups on using our tools. Facebook is committed to continuing to provide a platform where people can raise awareness about human rights abuses around the globe, and we have a track record of partnering with experts and local organizations on these issues. For example, we have been part of the Global Network Initiative (GNI) since 2013. That organization brings together industry, civil society, academics, and socially-responsible investors to address freedom-of-expression and privacy issues online. An independent assessor conducted a human-rights-impact assessment of Facebook to confirm that we comply with GNI's principles.

We are further strengthening our civil society partner network so that we have a better understanding of local context and challenges. We are focusing on digital literacy education with local partners in Myanmar and Sri Lanka. For example, we launched a local language version of our Community Standards (https://www.facebook.com/safety/resources/myanmar) to educate new users on how to use Facebook responsibly in 2015 and we have been promoting these actively in Myanmar, reaching over 8 million people through promotional posts on our platform alone. We've also rolled out several education programs and workshops with local partners to update them on our policies and tools so that they can use this information in outreach to communities around the country. One example of our education initiatives is our work with the team that developed the Panzagar initiative (https://www.facebook.com/supportflowerspeech) to develop the Panzagar counterspeech Facebook stickers to empower people in Myanmar to share positive messages online. We also recently released locally illustrated false news tips, which were promoted on Facebook and in consumer print publications. We have a dedicated Safety Page for Myanmar (https://www.facebook.com/safety/resources/myanmarand) and have delivered hard copies of our local language Community Standards and safety and security tips to civil society groups in Myanmar who have distributed them around the country for trainings. Similarly, in Sri Lanka, we ran a promotion in English, Sinhalese, and Tamil at the top of News Feeds in April 2018 to educate people on our Community Standards, in particular hate speech. The content has been viewed almost 10 million times by almost 4 million people.

Our Community Standards (https://www.facebook.com/communitystandards) prohibit hate speech that targets people based on their race, ethnic identity, or religion. We remove violating content when it is reported to us. We also have designated several hate figures and hate organizations in Myanmar. These include Wirathu, Thuseitta, Ma Ba Tha, and Parmaukkha. This means these individuals or organizations are not allowed a presence on Facebook, and we will remove accounts and content that support, praise or represent these individuals or organizations. In addition to removing content that violates our Community Standards or Page Terms, we disable the accounts of repeat infringers in appropriate circumstances. Over the last several

months, we have proactively searched for and removed content on the platform that praises, supports, or represents Wirathu.

8. In your testimony, you stated that Facebook will "have about 20,000 people at the company who work on security and content-review-related issues." Is this number sufficient to review all the information that is shared on Facebook by your over 2,000,000,000 users (meaning approximately I content reviewer for every 10,000 users)? When will these people be in place? What is being done to ensure they follow a standard protocol instead of being influenced by their personal biases?

Our effort to make our platform safer and more secure is a holistic one that involves a continual evaluation of our personnel, processes, and policies, and we make changes as appropriate.

We are doubling the size of our security and content review teams (from 10,000 to 20,000) over the course of this year. We currently have approximately 15,000 people working on these teams. Of that 15,000, more than 7,500 people review content around the world.

- Our content review team is global and reviews reports in over 50 languages.
- Reports are reviewed 24 hours a day, 7 days a week and the vast majority of reports are reviewed within 24 hours.
- Our goal is always to have the right number of skilled people with the right language capabilities to ensure incoming reports are reviewed quickly and efficiently.
- We hire people with native language and other specialist skills according to the needs we see from incoming reports.
- The team also includes specialists in areas like child safety, hate speech and counter-terrorism, software engineers to develop review systems, quality control managers, policy specialists, legal specialists, and general reviewers.
- To provide 24/7 coverage across dozens of languages and time zones and ensure that Facebook is a place where both expression and personal safety are protected and respected, our content review team includes a combination of employees, contractors, and vendor partners based in locations around the world. We partner with reputable vendors who are required to comply with specific obligations, including provisions for resiliency, support, transparency, and user privacy.

We are also using machine learning to better detect and action on content and people that should not be using our platform. For example, we incorporated learnings from interference in previous elections to better detect and stop false accounts from spreading misinformation in more recent elections. We recently shared how we are using machine learning to prevent bad actors like terrorists or scammers from using our platform (https://www.facebook.com/notes/facebook-security/introducing-new-machine-learning-techniques-to-help-stop-scams/10155213964780766/).

We believe that over the long term, building AI tools is the scalable way to identify and root out most content that violates our policies. We are making substantial investments in building and improving these tools. We already use artificial intelligence to help us identify threats of real world harm from terrorists and others. For example, the use of AI and other automation to stop the spread of terrorist content is showing promise. Today, 99 percent of the ISIS and Al Qaeda related terror content we remove from Facebook is content we detect before anyone in our community has flagged it to us, and in some cases, before it goes live on the site. We do this primarily through the use of automated systems like photo and video matching and text-based machine learning. We also use AI to help find child exploitation images, hate speech, discriminatory ads, and other prohibited content.

Our Community Standards are global and all reviewers use the same guidelines when making decisions. They undergo extensive training when they join and, thereafter, are regularly trained and tested with specific examples on how to uphold the Community Standards and take the correct action on a piece of content. This training includes when policies are clarified, or as they evolve. We seek to write actionable policies that clearly distinguish between violating and non-violating content and we seek to make the decision making process for reviewers as objective as possible.

Our reviewers are not working in an empty room. There are quality control mechanisms as well as management on site to help or seek guidance from if needed. When a reviewer isn't clear on the action to take based on the Community Standards, they can pass the content decision to another team for review. We also audit the accuracy of reviewer decisions on an ongoing basis to coach them and follow up on improving, where errors are being made. When we're made aware of incorrect content removals, we review them with our Community Operations team so as to prevent similar mistakes in the future.

We are introducing the right to appeal our decisions on individual posts so users can ask for a second opinion when they think we've made a mistake. As a first step, we are launching appeals for posts that were removed for nudity/sexual activity, hate speech or graphic violence. We are working to extend this process further, by supporting more violation types, giving people the opportunity to provide more context that could help us make the right decision, and making appeals available not just for content that was taken down, but also for content that was reported and left up. We believe giving people a voice in the process is another essential component of building a fair system.

9. On April 18th, Buzzfeed News published an exposé on the role Facebook plays in perpetrating sex trafficking. According to the article, even when confronted with these facts, Facebook did not react despite "promising that a representative would comment." Only after the article's publication did Facebook act and, ultimately, shut down that means of communication. How can we count on Facebook to ensure that this is not repeated? How can we count on Facebook to be proactive to issues instead of only reacting when publicly shamed? How can we count on Facebook to uphold legally-required privacy standards when you cannot uphold your own community standards?

Facebook is committed to making our platform a safe place, especially for individuals who may be vulnerable. We have a long history of working successfully with governments to address a wide variety of threats to our platform, including child exploitation. When we learn of a situation involving physical abuse, child exploitation, or an imminent threat of harm to a person, we immediately report the situation to first responders or the National Center for Missing and Exploited Children (NCMEC).

Further, as part of official investigations, government officials sometimes request data about people who use Facebook. We have processes in place to handle these government requests, and we disclose account records in accordance with our terms of service and applicable law. We also have a global team that strives to respond within minutes to emergency requests from law enforcement.

Our relationship with NCMEC also extends to an effort that we launched in 2015 to send AMBER Alerts to the Facebook community to help find missing children. When police determine that a case qualifies for an AMBER Alert, the alert is issued by the NCMEC and distributed through the Facebook system with any available information, including a photograph of the missing child, a license plate number, and the names and descriptions of the child and suspected abductor. Law enforcement determines the range of the target area for each alert. We know the chances of finding a missing child increase when more people are on the lookout, especially in the critical first hours. Our goal is to help get these alerts out quickly to the people who are in the best position to help, and a number of missing children have been found through AMBER Alerts on Facebook.

Further, we work tirelessly to identify and report child exploitation images (CEI) to appropriate authorities. We identify CEI through a combination of automated and manual review. On the automated review side, we use image hashing to identify known CEI. On the manual review side, we provide in-depth training to content reviewers on how to identify possible CEI. Confirmed CEI is reported to the NCMEC, which then forwards this information to appropriate authorities. When we report content to the NCMEC, we preserve account information in accordance with applicable law, which can help further law enforcement investigations. We also reach out to law enforcement authorities in serious cases to ensure that our reports are received and acted upon.

10. In every profession there is a code of professional responsibility, a code of ethics. Your industry has, so far, avoided these operating standards through self-regulation. Facebook's repeated and ongoing issues show that this is no longer feasible. In the digital age, what should a code of responsibility contain? Who should be responsible for enforcing it?

See Response to Question 3.

The Honorable Anna G. Eshoo

1. During your testimony at the House Energy and Commerce Committee, on April 11, 2018, I asked if you would be willing to change your business model to protect individual privacy, and you said you weren't "sure what that means."

a. As I understand your current business model, it relies at least in part on harvesting the personal data of its users and on targeted advertising. Is Facebook willing to fundamentally alter the volume and type of information it gathers and stores about its users and how it distributes it, in order to carry out *your stated commitment* to preserve privacy and democracy?

b. Explain in concise, plain language exactly what data of Facebook users is still being gathered and retained by Facebook, so that a user signing up for the first time would fully understand it?

Like many other free online services, we sell advertising space to third parties. Doing so enables us to offer our services to consumers for free. This is part of our mission to give people the power to build community and bring the world closer together.

As explained in our Data Policy, we collect three basic categories of data about people: (1) data about things people do and share (and who they connect with) on our services, (2) data about the devices people use to access our services, and (3) data we receive from partners, including the websites and apps that use our business tools. Our Data Policy provides more detail about each of the three categories.

We use this information for a variety of purposes, including to provide, personalize, and improve our products, provide measurement, analytics, and other business services, promote safety and security, to communicate with people who use our services, and to research and innovate to promote the social good. We provide more information in our Data Policy about these uses as well.

Our policies limit our retention of the data that we receive in several ways. Specifically, we store data until it is no longer necessary to provide our services and Facebook products, or until a person's account is deleted—whichever comes first. This is a case-by-case determination that depends on things like the nature of the data, why it is collected and processed, and relevant legal or operational retention needs. For example, if a user posts something on their Facebook profile, then that information would be retained until they delete it or until they delete their account.

In general, when a user deletes their account, we delete things they have posted, such as their photos and status updates, and they won't be able to recover that information later. (Information that others have shared about them isn't part of their account and won't be deleted.)

There are some limited exceptions to these policies: For instance, information can be accessed and preserved for an extended period when it is the subject of a legal request or obligation, governmental investigation, or investigations of possible violations of our terms or

policies, or otherwise to prevent harm. We also retain information from accounts disabled for terms violations for at least a year to prevent repeat abuse or other term violations.

In our ongoing efforts to identify ways that we can improve our privacy practices, we're building new experiences to help people understand how we collect and use data. This includes further restricting the data third-party app developers can ask people to share and announcing plans to build Clear History, a new feature that will enable users to see the websites and apps that send us information when they use them, clear this information from their accounts, and turn off our ability to store it associated with their accounts going forward.

2. Is Facebook willing to work with Congress and stakeholders to provide a blanket opt-in that is in transparent, clear, brief, pedestrian language that conveys to the user the full extent of where Facebook gets its data about us and who it shares that data with? (This should include not only what the user deliberately types into their profile, such as their hobbies or favorite books, but also data aggregated through posting and clicking articles, Liking friends' posts, etc.)

Facebook is generally not opposed to regulation but wants to ensure it is the right regulation. The issues facing the industry are complex, multi-faceted, and affect an important part of peoples' lives. As such, Facebook is absolutely committed to working with regulators, like Congress, to craft the right regulations. Facebook would be happy to review any proposed legislation and provide comments.

Our approach is to provide clear information to people about how their information is used and how they can control it. We agree that companies should provide clear and plain information about their use of data and strive to do this in our Data Policy, in in-product notices and education, and throughout our product—and we continuously work on improving this. We provide the same information about our data practices to users around the world and are required under many existing laws—including US laws (e.g., Section 5 of the FTC Act)—to describe our data practices in language that is fair and accurate.

3. Does Facebook now provide its users <u>real-time</u> access to the <u>complete</u> set of information it has on its users, including the sites from which they may have clicked through to Facebook? Are so consumers told when and where that data ends up with third parties? Does Facebook provide notification to the user as to how much of their data is being transmitted each time they click "agree"? If not, why not? Would Facebook object to providing more specific information to users?

We believe that it's important to communicate with people about the information that we collect and how people can control it. That is why we work hard to provide this information to people in a variety of ways: in our Data Policy, and in Privacy Basics, which provides walkthroughs of the most common privacy questions we receive. Beyond simply disclosing our practices, we also think it's important to give people access to their own information, which we do through our Download Your Information and Access Your Information tools, Activity Log, and Ad Preferences, all of which are accessible through our Privacy Shortcuts tool. We also provide information about these topics as people are using the Facebook service itself.

We've heard loud and clear that privacy settings and other important tools are too hard to find and that we must do more to keep people informed. So, we're taking additional steps to put people more in control of their privacy. For instance, we redesigned our entire settings menu on mobile devices from top to bottom to make things easier to find. We also created a new Privacy Shortcuts in a menu where users can control their data in just a few taps, with clearer explanations of how our controls work. The experience is now clearer, more visual, and easy-to-find. Furthermore, we also updated our terms of service that include our commitments to everyone using Facebook. We explain the services we offer in language that's easier to read. We also updated our Data Policy to better spell out what data we collect and how we use it in Facebook, Instagram, Messenger, and other products.

Our Download Your Information or "DYI" tool is Facebook's data portability tool and was launched many years ago to let people access and download many types of information that we maintain about them. The data in DYI and in our Ads Preferences tool contain each of the interest categories that are used to show people ads, along with information about the advertisers that are currently running ads based on their use of an advertiser's website or app. People also can choose not to see ads from those advertisers. We recently announced expansions to Download Your Information, which, among other things, will make it easier for people to see their data, delete it, and easily download and export it. More information is available at https://newsroom.fb.com/news/2018/04/new-privacy-protections/.

Responding to feedback that we should do more to provide information about websites and apps that send us information when people use them, we also announced plans to build Clear History. This new feature will enable users to see the websites and apps that send us information when they use them, clear this information from their account, and turn off Facebook's ability to store it associated with their account going forward.

We have also introduced Access Your Information. This feature provides a new way for people to access and manage their information. Users can go here to delete anything from their timeline or profile that they no longer want on Facebook. They can also see their ad interests, as well as information about ads they've clicked on and advertisers who have provided us with information about them that influence the ads they see. From here, they can go to their ad settings to manage how this data is used to show them ads.

4. Without an individual having signed up on Facebook, it appears Facebook is able to track them and create a ghost profile for the purposes of 'connecting people' (i.e. monetizing connections).

a. How does Facebook track and collect data on people who do not have Facebook accounts?

b. How much information do you already have on the typical user at the time they sign up for an account?

c. How do you treat the data of a person who has not yet to agreed Facebook's terms of service or privacy policy?

When people visit apps or websites that feature our technologies—like the Facebook Like or Comment button—our servers automatically log (i) standard browser or app records of the fact that a particular device or user visited the website or app (fthis connection to Facebook's servers occurs automatically when a person visits a website or app that contains our technologies, such as a Like button, and is an inherent function of internet design); and (ii) any additional information the publisher of the app or website chooses to share with Facebook about the person's activities on that site (such as the fact that a purchase was made on the site). This is a standard feature of the internet, and most websites and apps share this same information with multiple different third-parties whenever people visit their website or app. For example, the House Energy and Commerce Committee's website shares information with Google Analytics to help improve the site. This means that, when a person visits the Committee's website, it sends browser information about their visit to that third party. More information about how this works is available at https://newsroom.fb.com/news/2018/04/data-off-facebook/.

When the person visiting a website featuring Facebook's tools is not a registered Facebook user, Facebook does not have information identifying that individual, and it does not create profiles for this individual.

We use the browser and app logs that apps and websites send to us—described above—in the following ways for non-Facebook users. First, these logs are critical to protecting the security of Facebook and to detecting or preventing fake account access. For example, if a browser has visited hundreds of sites in the last five minutes, that's a sign the device might be a bot, which would be an important signal of a potentially inauthentic account if that browser then attempted to register for an account. Second, we aggregate those logs to provide summaries and insights to websites and apps about how many people visit or use their product, or use specific features like our Like button—but without providing any information about a specific person. We do not create profiles for non-Facebook users, nor do we use browser and app logs for non-Facebook users to show targeted ads from our advertisers to them or otherwise seek to personalize the content they see. However, we may take the opportunity to show a general ad that is unrelated to the attributes of the person or an ad encouraging the non-user to sign up for Facebook.

We do receive some information from devices and browsers that may be used by non-users. For example:

- We also may receive information about the device of a non-registered user if that user visits a part of Facebook that does not require people to log in—such as a public Facebook Page. The information we log when people visit our websites or apps is the same as described above and is the same information that any provider of an online service would receive.

- In addition, Facebook may receive some basic information about devices where Facebook apps are installed, including before people using those devices have registered for Facebook (such as when a user downloads a Facebook app, but has not yet created an account, or if the app is preloaded on a given device). This device data includes things like device model, operating system, IP address, app version and device identifiers. We use this information to provide the right version of the app, help people who want to create accounts (for example, optimizing the registration flow for the specific device),

retrieving bug fixes and measuring and improving app performance. We do not use this information to build profiles about non-registered users.

5. During your testimony I asked whether you were aware of other third party information mishandlings that have not been disclosed. You responded that you were "currently going through the process of investigating every single app that had access to a large amount of data" and that you imagine that "because there were tens of thousands of apps [you] will find some suspicious activity."

a. As of this date, have you determined whether misuse or misdistribution of data that violated the Facebook policies that third party apps had agreed to ever occurred with other apps?

We are in the process of investigating every app that had access to a large amount of information before we changed our Platform in 2014. The investigation process is in full swing, and it has two phases. First, a comprehensive review to identify every app that had access to this amount of Facebook data and to focus on apps that present reason for deeper investigation. And second, where we have concerns, we will conduct interviews, make requests for information (RFI)—which ask a series of detailed questions about the app and the data it has access to—and perform audits using expert firms that may include on-site inspections. We have large teams of internal and external experts working hard to investigate these apps as quickly as possible. As of early June 2018, thousands of apps have been investigated and around 200 apps have been suspended—pending a thorough investigation into whether they did in fact misuse any data. Where we find evidence that these or other apps did misuse data, we will ban them and let people know.

These apps relate to a handful of developers: Kogan, AIQ, Cube You, the Cambridge Psychometrics Center, and myPersonality, with many of the suspended apps being affiliated with the same entity. Many of these suspensions include apps that appear to be "test" apps that were never released to the public, and therefore would not have acquired significant user data, although our investigation into these apps is ongoing.

Additionally, we have suspended an additional 14 apps, which were installed by around one thousand people. They were all created after 2014, after we made changes to more tightly restrict our platform APIs to prevent abuse. However, these apps appear to be linked to AIQ, which was affiliated with Cambridge Analytica. So, we have suspended them while we investigate further. Any app that refuses to take part in or fails our audit will be banned.

b. How long do you estimate it will take to fully vet each app to determine whether a misuse has taken place?

It's going to take many months to do this full process.

c. Will you commit to notifying users as soon as Facebook determines that there has been a misuse or wrongful distribution of their data by third party apps?

Where we find evidence that these or other apps did misuse data, we will ban them from the platform and tell people who used or may have had data shared with the app.

d. In response to my question regarding Cambridge Analytica, you stated that you learned about the Cambridge Analytica breach in 2015. Why did it take until 2018 for the public to learn the full extent of the crisis?

When Facebook learned about Kogan's breach of Facebook's data use policies in December 2015, we took immediate action. The company retained an outside firm to assist in investigating Kogan's actions, to demand that Kogan and each party he had shared data with delete the data and any derivatives of the data, and to obtain certifications that they had done so. Because Kogan's app could no longer collect most categories of data due to changes in Facebook's platform, our highest priority at that time was ensuring deletion of the data that Kogan may have accessed before these changes took place. With the benefit of hindsight, we wish we had notified people whose information may have been impacted. Facebook has since notified all people potentially impacted with a detailed notice at the top of their News Feed.

6. Has Cambridge Analytica now fully complied with Facebook's "demands" to delete data obtained via Facebook and Mr. Kogan's app? If so, how can this be verified?

In March 2018, we learned from news reports that contrary to the certifications given, not all of the Kogan data may have been deleted by Cambridge Analytica. We have no direct evidence of this and no way to confirm this directly without accessing Cambridge Analytica's systems and conducting a forensic audit. We have held off on audits of Cambridge Analytica and other parties that are being investigated by the UK Information Commissioner's Office at its request. Our investigation is ongoing.

7. During my questioning I asked twice whether you spoke with Cambridge Analytica's CEO immediately following your knowledge of the misuse. You replied that you "got in touch" with "them" and the Chief Data Officer.

a. Did you in fact contact and speak with the principle executive of Cambridge Analytica immediately after you learned of the breach, and if not, why not? Have you done so since?

On December 11, 2015, *The Guardian* published an article reporting that Kogan and his company, GSR, may have passed information the app had obtained from Facebook users to SCL Elections Ltd. (SCL)/Cambridge Analytica. Kogan and his company violated Facebook's Platform Policies, which explicitly prohibited selling user data accessed from Facebook and from sharing any user data accessed from Facebook with any ad network, data broker or other advertising or monetization related service.

For this reason, Facebook immediately banned the app from our platform and investigated what happened and what further action we should take to enforce our Platform Policies. Facebook also contacted Kogan/GSR and demanded that they explain what data they collected, how they used it, and to whom they disclosed it. Facebook further insisted that Kogan and GSR, as well as other persons or entities to whom they had disclosed any such data, account for and irretrievably delete all such data and information.

Facebook also contacted Cambridge Analytica to investigate the allegations reflected in the reporting. On January 18, 2016, Cambridge Analytica provided written confirmation to Facebook that it had deleted the data received from Kogan and that its server did not have any backups of that data. On June 11, 2016, Kogan executed signed certifications of deletion on behalf of himself and GSR. The certifications also purported to identify all of the individuals and entities that had received data from GSR (in addition to Kogan and his lab), listing the following: SCL, Eunoia Technologies (a company founded by Christopher Wylie), and a researcher at the Toronto Laboratory for Social Neuroscience at the University of Toronto. On July 7, 2016, a representative of the University of Toronto certified that it deleted any user data or user-derived data. On August 16, 2016, Eunoia (executed by Eunoia Founder Christopher Wylie) certified that it deleted any user and user-derived data. On September 6, 2016, counsel for SCL informed counsel for Facebook that SCL had permanently deleted all Facebook data and derivative data received from GSR and that this data had not been transferred or sold to any other entity. On April 3, 2017, Alexander Nix, on behalf of SCL, certified to Facebook, that it deleted the information that it received from GSR or Kogan.

Because all of these concerns relate to activity that took place off of Facebook and its systems, we have no way to confirm whether Cambridge Analytica may have Facebook data without conducting a forensic audit of its systems. Cambridge Analytica has agreed to submit to a forensic audit, but we have not commenced that yet due to a request from the UK Information Commissioner's Office, which is simultaneously investigating Cambridge Analytica (which is based in the UK). And even with an audit, it may not be possible to determine conclusively what data was shared with Cambridge Analytica or whether it retained data after the date it certified that data had been deleted.

8. It is documented that the Trump Campaign paid Facebook millions of dollars for advertising in 2016 in advance of the presidential election. It also has been acknowledged that Facebook had a team embedded at the Trump Campaign's digital operations center. Did Facebook know during this period that Cambridge Analytica was a data vendor for the Trump Campaign? If so, why did Facebook not object to working with the Trump Campaign in this way, considering the data company it was working with – Cambridge Analytica – had been known by Facebook by this time to have violated its own agreement with Facebook?

While no one from Facebook was assigned full-time to the Trump campaign, Facebook employees did interact with Cambridge Analytica employees. Our investigation is ongoing and our review indicates that Facebook employees did not identify any issues involving the improper use of Facebook data in the course of their interactions with Cambridge Analytica during the 2016 US Presidential campaign.

The week prior to your appearance before the House Energy and Commerce Committee, I surveyed my constituents and asked them to submit one question they would ask you if given the opportunity. I received the following responses and I'm including them here and I ask you to respond to each of them:

9. What reparations will Facebook give the American people for allowing this breach of our democracy on your platform, and what is the timeline to complete them?

We want our platform to be a place where people can have authentic conversations about elections and other political topics. We believe this kind of engagement promotes democracy, but we know that there are actors working to interfere with those conversations and undermine our elections. We are already taking steps to proactively prevent election interference and we are strengthening these protections going forward.

Engagement with campaigns: We want all candidates, groups, and voters to use our platform to engage in elections. We want it to be easy for people to find, follow, and contact their elected representatives—and those running to represent them. That's why, for candidates across the political spectrum, Facebook offers the same levels of support in key moments to help campaigns understand how best to use the platform. Both the Obama and Romney campaigns had access to the same tools, and no campaign received any special treatment from Facebook. Likewise, we offered identical support to both the Trump and Clinton campaigns, and had teams assigned to both. Everyone had access to the same tools, which are the same tools that every campaign is offered, and is consistent with support provided to commercial clients in the normal course of business. Facebook representatives advise political advertisers on Facebook, as they would with other, non-political managed accounts. We have a compliance team that trains our sales representatives to comply with all federal election law requirements in this area.

While no one from Facebook was assigned full-time to the Trump campaign, Facebook employees did interact with Cambridge Analytica employees. While our investigation is ongoing, our review indicates that Facebook employees did not identify any issues involving the improper use of Facebook data in the course of their interactions with Cambridge Analytica during the 2016 US Presidential campaign.

Election Integrity: In the run-up to the 2016 elections, we were focused on the kinds of cybersecurity attacks typically used by nation states, for example phishing and malware attacks. And we were too slow to spot information operations interference. Since then, we've made important changes to prevent bad actors from using misinformation to undermine the democratic process. This will never be a solved problem because we're up against determined, creative and well-funded adversaries. But we are making steady progress. Here is a list of the 10 most important changes we have made:

- **Ads transparency.** Advertising should be transparent: users should be able to see all the ads an advertiser is currently running on Facebook, Instagram and Messenger. And for ads with political content, we've created an archive that will hold ads with political content for seven years—including information about ad impressions and spend, as well as demographic data such as age, gender and location. People in Canada and Ireland have already been able to see all the ads that a Page is running on Facebook—and we've launched this globally.

- **Verification and labeling.** Every advertiser will now need to confirm their ID and location before being able to run any ads with political content in the US. All ads with political content will also clearly state who paid for them.

- **Updating targeting.** We want ads on Facebook to be safe and civil. We thoroughly review the targeting criteria advertisers can use to ensure they are

consistent with our principles. As a result, we removed nearly one-third of the targeting segments used by the IRA. We continue to allow some criteria that people may find controversial. But we do see businesses marketing things like historical books, documentaries or television shows using them in legitimate ways.

- **Better technology.** Over the past year, we've gotten increasingly better at finding and disabling fake accounts. We now block millions of fake accounts each day as people try to create them—and before they've done any harm. This is thanks to improvements in machine learning and artificial intelligence, which can proactively identify suspicious behavior at a scale that was not possible before—without needing to look at the content itself.

- **Action to tackle fake news.** We are working hard to stop the spread of false news. We work with third-party fact-checking organizations to limit the spread of articles rated false. To reduce the spread of false news, we remove fake accounts and disrupt economic incentives for traffickers of misinformation. We also use various signals, including feedback from our community, to identify potential false news. In countries where we have partnerships with independent third-party fact-checkers, stories rated as false by those fact-checkers are shown lower in News Feed. If Pages or domains repeatedly create or share misinformation, we significantly reduce their distribution and remove their advertising rights. We also want to empower people to decide for themselves what to read, trust, and share. We promote news literacy and work to inform people with more context. For example, if third-party fact-checkers write articles about a news story, we show them immediately below the story in the Related Articles unit. We also notify people and Page Admins if they try to share a story, or have shared one in the past, that's been determined to be false. In addition to our own efforts, we're learning from academics, scaling our partnerships with third-party fact-checkers and talking to other organizations about how we can work together.

  A key focus is working to disrupt the economics of fake news. For example, preventing the creation of fake accounts that spread it, banning sites that engage in this behavior from using our ad products, and demoting articles found to be false by fact checkers in News Feed—causing it to lose 80% of its traffic. We now work with independent fact checkers in the US, France, Germany, Ireland, the Netherlands, Italy, Mexico, Colombia, India, Indonesia and the Philippines with plans to scale to more countries in the coming months.

- **Significant investments in security.** We're doubling the number of people working on safety and security from 10,000 last year to over 20,000 this year. We expect these investments to impact our profitability. But the safety of people using Facebook needs to come before profit.

- **Industry collaboration.** Recently, we joined 34 global tech and security companies in signing a TechAccord pact to help improve security for everyone.

- **Information sharing and reporting channels.** In the 2017 German elections, we worked closely with the authorities there, including the Federal Office for Information Security (BSI). This gave them a dedicated reporting channel for security issues related to the federal elections.

- **Tracking 40+ elections.** In recent months, we've started to deploy new tools and teams to proactively identify threats in the run-up to specific elections. We first tested this effort during the Alabama Senate election, and plan to continue these efforts for elections around the globe, including the US midterms. Last year we used public service announcements to help inform people about fake news in 21 separate countries, including in advance of French, Kenyan and German elections.

- **Action against the Russia-based IRA.** In April, we removed 70 Facebook and 65 Instagram accounts—as well as 138 Facebook Pages—controlled by the IRA primarily targeted either at people living in Russia or Russian-speakers around the world including from neighboring countries like Azerbaijan, Uzbekistan and Ukraine. The IRA has repeatedly used complex networks of inauthentic accounts to deceive and manipulate people in the US, Europe and Russia—and we don't want them on Facebook anywhere in the world.

10. My family wants to know why Facebook's policies on unacceptable speech weren't adhered to. Slander and lies ARE NOT free speech.

Freedom of expression is one of our core values, and we believe that adding voices to the conversation creates a richer and more vibrant community. We want people to feel confident that our community welcomes all viewpoints and we are committed to designing our products to give all people a voice and foster the free flow of ideas and culture. We recognize how important it is for Facebook to be a place where people feel empowered to communicate, and we take our role in keeping abuse off our service seriously. Our mission entails embracing diverse views. We err on the side of allowing content, even when some find it objectionable, unless removing that content prevents a specific harm.

However, we are, first and foremost, a technology company. Facebook does not create or edit the content that our users post on our platform. While we seek to be a platform for a broad range of ideas, we do moderate content in good faith according to published community standards in order to keep users on the platform safe, reduce objectionable content and to make sure users participate on the platform responsibly.

11. You said you would get a notice to users affected by Cambridge Analytica. That notice has yet to arrive, and you should have known it was expected before this hearing. Please explain what measures you will take to prevent such high-profile failures in the future.

Facebook's policies regarding third-party usage of its platform technologies have prohibited—and continue to prohibit—third-party app developers from selling or licensing user data accessed from Facebook and from sharing any user data accessed from Facebook with any ad network, data broker or other advertising or monetization-related service. We take action on

potential violations of our Platform Policies based on proactive review, external reports, and other signals. Kogan was not permitted to sell or transfer data to third-parties for the purposes he did. In doing so, Kogan and his company violated Facebook's Platform Policies.

On December 11, 2015, *The Guardian* published an article reporting that Kogan and his company, GSR, may have passed information the app had obtained from Facebook users to SCL Elections Ltd. (SCL)/Cambridge Analytica. Facebook immediately banned Kogan's app from our platform and investigated what happened and what further action Facebook should take to enforce our Platform Policies. Facebook considered the matter closed after obtaining written certifications and confirmations from Kogan, GSR, Cambridge Analytica, and SCL declaring that all such data they had obtained was accounted for and destroyed. We did not have any reason to affirmatively question the veracity of any of these certifications until March 2018, when we learned from media reporting that questions had been raised concerning the accuracy of the certifications. Facebook immediately banned Cambridge Analytica and SCL from purchasing advertisements on our services as well as removed the personal accounts of some of their officers. Moreover, while Facebook's policies in place at the time allowed us to audit apps to ensure that they were safe and did not violate its terms, we had already terminated Kogan's app's access to Facebook. Accordingly, there were no ongoing concerns about the level of data that app could access or might access in the future. With the benefit of hindsight, we wish we had notified people whose information may have been impacted. Facebook has since notified all people potentially impacted with a detailed notice at the top of their News Feed.

12. What specifically will be done to inform users of how data about them will be used?

Facebook's policies regarding third-party usage of its platform technologies have prohibited—and continue to prohibit—third-party app developers from selling or licensing user data obtained from Facebook and from sharing any user data obtained from Facebook with any ad network, data broker or other advertising or monetization-related service.

We use a variety of tools to enforce Facebook policies against violating parties, including developers. We review tens of thousands of apps per year and regularly disapprove noncompliant apps as part of our proactive review process. We also use tools like cease and desist letters, account suspensions, letter agreements, and civil litigation. For example, since 2006, Facebook has sent over 1,150 cease-and-desist letters to over 1,600 targets. In 2017, we took action against about 370,000 apps, ranging from imposing certain restrictions to removal of the app from the platform. Moreover, we have required parties who have procured our data without authorization to delete that data. We have invested significant resources in these efforts.

Recently, we announced a number of additional steps we're taking to address concerns raised by Kogan's app.

- **Review our platform.** We will investigate all apps that had access to large amounts of data before the platform changes we announced in 2014, and we will audit any app where we identify suspicious activity. If we identify misuses of data, we'll take immediate action, including banning the app from our platform and pursuing legal action if appropriate.

- **Tell people about data misuse.** We will tell people about apps that have misused their data. This includes building a way for people to know if their data might have been accessed via the app. Moving forward, if we remove an app, we will tell people.

- **Turn off access for unused apps.** If someone has not used an app within the last three months, we will turn off the app's access to their data.

- **Restrict Facebook Login data.** We are changing Login, so that the only data that an app can request without app review will include name, profile photo, and email address. Requesting any other data will require approval from Facebook. We will also no longer allow apps to ask for access to information like religious or political views, relationship status and details, custom friends lists, education and work history, fitness activity, book reading and music listening activity, news reading, video watch activity, and games activity. We will encourage people to manage the apps they use. We already show people what apps their accounts are connected to and allow them to control what data they've permitted those apps to use. But we're making it easier for people to see what apps they use and the information they have shared with those apps.

- **Reward people who find vulnerabilities.** We launched the Data Abuse Bounty program so that people can report to us any misuses of data by app developers.

- **Update our policies.** We have updated our terms and Data Policy to explain how we use data and how data is shared with app developers.

13. What would restorative justice look like for all those harmed and impacted?

Facebook's policies regarding third-party usage of its platform technologies have prohibited—and continue to prohibit—third-party app developers from selling or licensing user data obtained from Facebook and from sharing any user data obtained from Facebook with any ad network, data broker or other advertising or monetization-related service.

We use a variety of tools to enforce Facebook policies against violating parties, including developers. We review tens of thousands of apps per year and regularly disapprove noncompliant apps as part of our proactive review process. We also use tools like cease and desist letters, account suspensions, letter agreements, and civil litigation. For example, since 2006, Facebook has sent over 1,150 cease-and-desist letters to over 1,600 targets. In 2017, we took action against about 370,000 apps, ranging from imposing certain restrictions to removal of the app from the platform. Moreover, we have required parties who have procured our data without authorization to delete that data. We have invested significant resources in these efforts.

Recently, we announced a number of additional steps we're taking to address concerns raised by Kogan's app.

- **Review our platform.** We will investigate all apps that had access to large amounts of data before the platform changes we announced in 2014, and we will audit any app where we identify suspicious activity. If we identify misuses of data, we'll take

immediate action, including banning the app from our platform and pursuing legal action if appropriate.

- **Tell people about data misuse.** We will tell people about apps that have misused their data. This includes building a way for people to know if their data might have been accessed via the app. Moving forward, if we remove an app, we will tell people.

- **Turn off access for unused apps.** If someone has not used an app within the last three months, we will turn off the app's access to their data.

- **Restrict Facebook Login data.** We are changing Login, so that the only data that an app can request without app review will include name, profile photo, and email address. Requesting any other data will require approval from Facebook. We will also no longer allow apps to ask for access to information like religious or political views, relationship status and details, custom friends lists, education and work history, fitness activity, book reading and music listening activity, news reading, video watch activity, and games activity. We will encourage people to manage the apps they use. We already show people what apps their accounts are connected to and allow them to control what data they've permitted those apps to use. But we're making it easier for people to see what apps they use and the information they have shared with those apps.

- **Reward people who find vulnerabilities.** We launched the Data Abuse Bounty program so that people can report to us any misuses of data by app developers.

- **Update our policies.** We have updated our terms and Data Policy to explain how we use data and how data is shared with app developers.

14. What actions have you taken with those responsible for allowing third party access to user's information?

Facebook's policies regarding third-party usage of its platform technologies have prohibited—and continue to prohibit—third-party app developers from selling or licensing user data obtained from Facebook and from sharing any user data obtained from Facebook with any ad network, data broker or other advertising or monetization-related service.

We use a variety of tools to enforce Facebook policies against violating parties, including developers. We review tens of thousands of apps per year and regularly disapprove noncompliant apps as part of our proactive review process. We also use tools like cease and desist letters, account suspensions, letter agreements, and civil litigation. For example, since 2006, Facebook has sent over 1,150 cease-and-desist letters to over 1,600 targets. In 2017, we took action against about 370,000 apps, ranging from imposing certain restrictions to removal of the app from the platform. Moreover, we have required parties who have procured our data without authorization to delete that data. We have invested significant resources in these efforts.

Recently, we announced a number of additional steps we're taking to address concerns raised by Kogan's app.

- **Review our platform.** We will investigate all apps that had access to large amounts of data before the platform changes we announced in 2014, and we will audit any app where we identify suspicious activity. If we identify misuses of data, we'll take immediate action, including banning the app from our platform and pursuing legal action if appropriate.

- **Tell people about data misuse.** We will tell people about apps that have misused their data. This includes building a way for people to know if their data might have been accessed via the app. Moving forward, if we remove an app, we will tell people.

- **Turn off access for unused apps.** If someone has not used an app within the last three months, we will turn off the app's access to their data.

- **Restrict Facebook Login data.** We are changing Login, so that the only data that an app can request without app review will include name, profile photo, and email address. Requesting any other data will require approval from Facebook. We will also no longer allow apps to ask for access to information like religious or political views, relationship status and details, custom friends lists, education and work history, fitness activity, book reading and music listening activity, news reading, video watch activity, and games activity. We will encourage people to manage the apps they use. We already show people what apps their accounts are connected to and allow them to control what data they've permitted those apps to use. But we're making it easier for people to see what apps they use and the information they have shared with those apps.

- **Reward people who find vulnerabilities.** We launched the Data Abuse Bounty program so that people can report to us any misuses of data by app developers.

- **Update our policies.** We have updated our terms and Data Policy to explain how we use data and how data is shared with app developers.

15. Can you guarantee that a similar or comparable breach will not happen again? Explain why.

Facebook's policies regarding third-party usage of its platform technologies have prohibited—and continue to prohibit—third-party app developers from selling or licensing user data obtained from Facebook and from sharing any user data obtained from Facebook with any ad network, data broker or other advertising or monetization-related service.

We use a variety of tools to enforce Facebook policies against violating parties, including developers. We review tens of thousands of apps per year and regularly disapprove noncompliant apps as part of our proactive review process. We also use tools like cease and desist letters, account suspensions, letter agreements, and civil litigation. For example, since 2006, Facebook has sent over 1,150 cease-and-desist letters to over 1,600 targets. In 2017, we took action against about 370,000 apps, ranging from imposing certain restrictions to removal of the app from the platform. Moreover, we have required parties who have procured our data without authorization to delete that data. We have invested significant resources in these efforts.

Recently, we announced a number of additional steps we're taking to address concerns raised by Kogan's app.

- **Review our platform.** We will investigate all apps that had access to large amounts of data before the platform changes we announced in 2014, and we will audit any app where we identify suspicious activity. If we identify misuses of data, we'll take immediate action, including banning the app from our platform and pursuing legal action if appropriate.

- **Tell people about data misuse.** We will tell people about apps that have misused their data. This includes building a way for people to know if their data might have been accessed via the app. Moving forward, if we remove an app, we will tell people.

- **Turn off access for unused apps.** If someone has not used an app within the last three months, we will turn off the app's access to their data.

- **Restrict Facebook Login data.** We are changing Login, so that the only data that an app can request without app review will include name, profile photo, and email address. Requesting any other data will require approval from Facebook. We will also no longer allow apps to ask for access to information like religious or political views, relationship status and details, custom friends lists, education and work history, fitness activity, book reading and music listening activity, news reading, video watch activity, and games activity. We will encourage people to manage the apps they use. We already show people what apps their accounts are connected to and allow them to control what data they've permitted those apps to use. But we're making it easier for people to see what apps they use and the information they have shared with those apps.

- **Reward people who find vulnerabilities.** We launched the Data Abuse Bounty program so that people can report to us any misuses of data by app developers.

- **Update our policies.** We have updated our terms and Data Policy to explain how we use data and how data is shared with app developers.

16. What specific policies and strategies do you intend to protect the privacy of Facebook users and give them control over what gets shared and with whom?

We believe everyone deserves good privacy controls. A user owns the information they share on Facebook. This means they decide what they share and who they share it with on Facebook, and they can change their mind. We require websites and apps who use our tools to tell users they're collecting and sharing their information with us, and to get users' permission to do so.

Everyone has the right to expect strong protections for their information. We also need to do our part to help keep our community safe, in a way that's consistent with people's privacy expectations. We've recently announced several steps to give people more control over their privacy, including a new Privacy Shortcuts tool that we're rolling out now to give people

information about how to control their information, including choosing who can see what they post and adding protections like two-factor authentication to their account. People can learn more about how to protect their privacy in our updated Data Policy and in our Privacy Basics feature (https://www.facebook.com/about/basics).

We are in the process of investigating every app that had access to a large amount of information before we changed our Platform in 2014. The investigation process is in full swing. We have large teams of internal and external experts working hard to investigate these apps as quickly as possible. As of early June 2018, thousands of apps have been investigated and around 200 apps have been suspended—pending a thorough investigation into whether they did in fact misuse any data. Where we find evidence that these or other apps did misuse data, we will ban them and let people know.

Facebook is generally not opposed to regulation but wants to ensure it is the right regulation. The issues facing the industry are complex, multi-faceted, and affect an important part of peoples' lives. As such, Facebook is absolutely committed to working with regulators, like Congress, to craft the right regulations. Facebook would be happy to review any proposed legislation and provide comments.

17. What will Facebook do THIS time to insure that this doesn't happen again? (Similar issues in 2010.)

Facebook's policies regarding third-party usage of its platform technologies have prohibited—and continue to prohibit—third-party app developers from selling or licensing user data obtained from Facebook and from sharing any user data obtained from Facebook with any ad network, data broker or other advertising or monetization-related service.

We use a variety of tools to enforce Facebook policies against violating parties, including developers. We review tens of thousands of apps per year and regularly disapprove noncompliant apps as part of our proactive review process. We also use tools like cease and desist letters, account suspensions, letter agreements, and civil litigation. For example, since 2006, Facebook has sent over 1,150 cease-and-desist letters to over 1,600 targets. In 2017, we took action against about 370,000 apps, ranging from imposing certain restrictions to removal of the app from the platform. Moreover, we have required parties who have procured our data without authorization to delete that data. We have invested significant resources in these efforts.

Recently, we announced a number of additional steps we're taking to address concerns raised by Kogan's app.

- **Review our platform.** We will investigate all apps that had access to large amounts of data before the platform changes we announced in 2014, and we will audit any app where we identify suspicious activity. If we identify misuses of data, we'll take immediate action, including banning the app from our platform and pursuing legal action if appropriate.

- **Tell people about data misuse.** We will tell people about apps that have misused their data. This includes building a way for people to know if their data might have been accessed via the app. Moving forward, if we remove an app, we will tell people.

- **Turn off access for unused apps.** If someone has not used an app within the last three months, we will turn off the app's access to their data.

- **Restrict Facebook Login data.** We are changing Login, so that the only data that an app can request without app review will include name, profile photo, and email address. Requesting any other data will require approval from Facebook. We will also no longer allow apps to ask for access to information like religious or political views, relationship status and details, custom friends lists, education and work history, fitness activity, book reading and music listening activity, news reading, video watch activity, and games activity. We will encourage people to manage the apps they use. We already show people what apps their accounts are connected to and allow them to control what data they've permitted those apps to use. But we're making it easier for people to see what apps they use and the information they have shared with those apps.

- **Reward people who find vulnerabilities.** We launched the Data Abuse Bounty program so that people can report to us any misuses of data by app developers.

- **Update our policies.** We have updated our terms and Data Policy to explain how we use data and how data is shared with app developers.

18. How do you plan to change your company's policy on transparency and WHEN will we see those changes?

We believe everyone deserves good privacy controls. A user owns the information they share on Facebook. This means they decide what they share and who they share it with on Facebook, and they can change their mind. We require websites and apps who use our tools to tell users they're collecting and sharing their information with us, and to get users' permission to do so.

Everyone has the right to expect strong protections for their information. We also need to do our part to help keep our community safe, in a way that's consistent with people's privacy expectations. We've recently announced several steps to give people more control over their privacy, including a new Privacy Shortcuts tool that we're rolling out now to give people information about how to control their information, including choosing who can see what they post and adding protections like two-factor authentication to their account. People can learn more about how to protect their privacy in our updated Data Policy and in our Privacy Basics feature (https://www.facebook.com/about/basics).

We are in the process of investigating every app that had access to a large amount of information before we changed our Platform in 2014. The investigation process is in full swing. We have large teams of internal and external experts working hard to investigate these apps as quickly as possible. As of early June 2018, thousands of apps have been investigated and around

200 apps have been suspended—pending a thorough investigation into whether they did in fact misuse any data. Where we find evidence that these or other apps did misuse data, we will ban them and let people know.

Facebook is generally not opposed to regulation but wants to ensure it is the right regulation. The issues facing the industry are complex, multi-faceted, and affect an important part of peoples' lives. As such, Facebook is absolutely committed to working with regulators, like Congress, to craft the right regulations. Facebook would be happy to review any proposed legislation and provide comments.

19. What are Facebook's guidelines on valuing users and customers, and how are they implemented?

As discussed with your staff, this question is not germane to the hearing.

20. Are you willing to state specific policies FB will implement to prevent a similar travesty?

We believe everyone deserves good privacy controls. A user owns the information they share on Facebook. This means they decide what they share and who they share it with on Facebook, and they can change their mind. We require websites and apps who use our tools to tell users they're collecting and sharing their information with us, and to get users' permission to do so.

Everyone has the right to expect strong protections for their information. We also need to do our part to help keep our community safe, in a way that's consistent with people's privacy expectations. We've recently announced several steps to give people more control over their privacy, including a new Privacy Shortcuts tool that we're rolling out now to give people information about how to control their information, including choosing who can see what they post and adding protections like two-factor authentication to their account. People can learn more about how to protect their privacy in our updated Data Policy and in our Privacy Basics feature (https://www.facebook.com/about/basics).

We are in the process of investigating every app that had access to a large amount of information before we changed our Platform in 2014. The investigation process is in full swing. We have large teams of internal and external experts working hard to investigate these apps as quickly as possible. As of early June 2018, thousands of apps have been investigated and around 200 apps have been suspended—pending a thorough investigation into whether they did in fact misuse any data. Where we find evidence that these or other apps did misuse data, we will ban them and let people know.

Facebook is generally not opposed to regulation but wants to ensure it is the right regulation. The issues facing the industry are complex, multi-faceted, and affect an important part of peoples' lives. As such, Facebook is absolutely committed to working with regulators, like Congress, to craft the right regulations. Facebook would be happy to review any proposed legislation and provide comments.

21. What is Facebook doing to protect my data now? And how is Facebook planning on making amends?

We believe everyone deserves good privacy controls. A user owns the information they share on Facebook. This means they decide what they share and who they share it with on Facebook, and they can change their mind. We require websites and apps who use our tools to tell users they're collecting and sharing their information with us, and to get users' permission to do so.

Everyone has the right to expect strong protections for their information. We also need to do our part to help keep our community safe, in a way that's consistent with people's privacy expectations. We've recently announced several steps to give people more control over their privacy, including a new Privacy Shortcuts tool that we're rolling out now to give people information about how to control their information, including choosing who can see what they post and adding protections like two-factor authentication to their account. People can learn more about how to protect their privacy in our updated Data Policy and in our Privacy Basics feature (https://www.facebook.com/about/basics).

We are in the process of investigating every app that had access to a large amount of information before we changed our Platform in 2014. The investigation process is in full swing. We have large teams of internal and external experts working hard to investigate these apps as quickly as possible. As of early June 2018, thousands of apps have been investigated and around 200 apps have been suspended—pending a thorough investigation into whether they did in fact misuse any data. Where we find evidence that these or other apps did misuse data, we will ban them and let people know.

Facebook is generally not opposed to regulation but wants to ensure it is the right regulation. The issues facing the industry are complex, multi-faceted, and affect an important part of peoples' lives. As such, Facebook is absolutely committed to working with regulators, like Congress, to craft the right regulations. Facebook would be happy to review any proposed legislation and provide comments.

22. What can Facebook do to prevent and deter the malicious third parties from using and selling the data they accessed and can now provide this data to other third parties?

Facebook's policies regarding third-party usage of its platform technologies have prohibited—and continue to prohibit—third-party app developers from selling or licensing user data obtained from Facebook and from sharing any user data obtained from Facebook with any ad network, data broker or other advertising or monetization-related service.

We use a variety of tools to enforce Facebook policies against violating parties, including developers. We review tens of thousands of apps per year and regularly disapprove noncompliant apps as part of our proactive review process. We also use tools like cease and desist letters, account suspensions, letter agreements, and civil litigation. For example, since 2006, Facebook has sent over 1,150 cease-and-desist letters to over 1,600 targets. In 2017, we took action against about 370,000 apps, ranging from imposing certain restrictions to removal of the app from the

platform. Moreover, we have required parties who have procured our data without authorization to delete that data. We have invested significant resources in these efforts.

Recently, we announced a number of additional steps we're taking to address concerns raised by Kogan's app.

- **Review our platform.** We will investigate all apps that had access to large amounts of data before the platform changes we announced in 2014, and we will audit any app where we identify suspicious activity. If we identify misuses of data, we'll take immediate action, including banning the app from our platform and pursuing legal action if appropriate.

- **Tell people about data misuse.** We will tell people about apps that have misused their data. This includes building a way for people to know if their data might have been accessed via the app. Moving forward, if we remove an app, we will tell people.

- **Turn off access for unused apps.** If someone has not used an app within the last three months, we will turn off the app's access to their data.

- **Restrict Facebook Login data.** We are changing Login, so that the only data that an app can request without app review will include name, profile photo, and email address. Requesting any other data will require approval from Facebook. We will also no longer allow apps to ask for access to information like religious or political views, relationship status and details, custom friends lists, education and work history, fitness activity, book reading and music listening activity, news reading, video watch activity, and games activity. We will encourage people to manage the apps they use. We already show people what apps their accounts are connected to and allow them to control what data they've permitted those apps to use. But we're making it easier for people to see what apps they use and the information they have shared with those apps.

- **Reward people who find vulnerabilities.** We launched the Data Abuse Bounty program so that people can report to us any misuses of data by app developers.

- **Update our policies.** We have updated our terms and Data Policy to explain how we use data and how data is shared with app developers.

23. How will Facebook give users control of personal data's use?

We believe that it's important to communicate with people about the information that we collect and how people can control it. As explained in our Data Policy, we collect three basic categories of data about people:

(1) data about things people do and share (and who they connect with) on our services;

(2) data about the devices people use to access our services; and

(3) data we receive from partners, including the websites and apps that use our business tools.

We collect information about the people, Pages, accounts, hashtags, and groups users are connected to and how they interact with them across our Products, such as people a user communicates with the most or groups users are part of. We also collect contact information if they choose to upload, sync, or import it from a device (such as an address book or call log or SMS log history), which we use for things like helping them and others find people they may know.

The data we use to show ads to people depends on the data we have received from people. For people who are new to Facebook, we may have minimal data that we can use. For people who have used our services for longer, we likely have more data, but the amount of data will depend on the nature of that use and how they have used our controls. Any person can see each of the specific interests we maintain about them for advertising by visiting Ads Preferences, which lets people see what interests we use to choose ads for them—and to edit or delete these interests. We also provide more detailed information about how we use data to decide what ads to show to people in our "About Facebook Ads" page, at https://www.facebook.com/ads/about. And, we do not sell people's information to anyone, and we never will.

All users must expressly consent to Facebook's Terms and Data Policy when registering for Facebook. The Data Policy explains the kinds of information we collect, how we use this information, how we share this information, and how users can manage and delete information.

Facebook does not create profiles for people without a Facebook account, but we do receive some information from devices and browsers that may be used by non-users. For example:

- When people visit apps or websites that feature our technologies—like the Facebook Like or Comment button—our servers automatically log (i) standard browser or app records of the fact that a particular device or user visited the website or app (this connection to Facebook's servers occurs automatically when a person visits a website or app that contains our technologies, such as a Like button, and is an inherent function of Internet design); and (ii) any additional information the publisher of the app or website chooses to share with Facebook about the person's activities on that site (such as the fact that a purchase was made on the site). This is a standard feature of the Internet, and most websites and apps share this same information with multiple different third-parties whenever people visit their website or app. When the person visiting a website featuring Facebook's tools is not a registered Facebook user, Facebook does not have information identifying that individual, and it does not create profiles for this individual.

- We also may receive information about the device of a non-registered user if that user visits a part of Facebook that does not require people to log in—such as a public Facebook Page. The information we log when people visit our websites or apps is the same as described above and is the same information that any provider of an online service would receive.

- In addition, Facebook may receive some basic information about devices where Facebook apps are installed, including before people using those devices have registered for Facebook (such as when a user downloads a Facebook app, but has not yet created an account, or if the app is preloaded on a given device). This device data includes things like device model, operating system, IP address, app version and device identifiers. We use this information to provide the right version of the app, help people who want to create accounts (for example, optimizing the registration flow for the specific device), retrieving bug fixes and measuring and improving app performance. We do not use this information to build profiles about non-registered users.

24. Will Facebook offer its members a blanket opt-out of the sharing of all personal information?

We believe everyone deserves good privacy controls. A user owns the information they share on Facebook. This means they decide what they share and who they share it with on Facebook, and they can change their mind. We require websites and apps who use our tools to tell users they're collecting and sharing their information with us, and to get users' permission to do so.

Everyone has the right to expect strong protections for their information. We also need to do our part to help keep our community safe, in a way that's consistent with people's privacy expectations. We've recently announced several steps to give people more control over their privacy, including a new Privacy Shortcuts tool that we're rolling out now to give people information about how to control their information, including choosing who can see what they post and adding protections like two-factor authentication to their account. People can learn more about how to protect their privacy in our updated Data Policy and in our Privacy Basics feature (https://www.facebook.com/about/basics).

We are in the process of investigating every app that had access to a large amount of information before we changed our Platform in 2014. The investigation process is in full swing. We have large teams of internal and external experts working hard to investigate these apps as quickly as possible. As of early June 2018, thousands of apps have been investigated and around 200 apps have been suspended—pending a thorough investigation into whether they did in fact misuse any data. Where we find evidence that these or other apps did misuse data, we will ban them and let people know.

Facebook is generally not opposed to regulation but wants to ensure it is the right regulation. The issues facing the industry are complex, multi-faceted, and affect an important part of peoples' lives. As such, Facebook is absolutely committed to working with regulators, like Congress, to craft the right regulations. Facebook would be happy to review any proposed legislation and provide comments.

25. What is his plan to prevent such data breaches in the future to keep users safe?

Facebook's policies regarding third-party usage of its platform technologies have prohibited—and continue to prohibit—third-party app developers from selling or licensing user

data obtained from Facebook and from sharing any user data obtained from Facebook with any ad network, data broker or other advertising or monetization-related service.

We use a variety of tools to enforce Facebook policies against violating parties, including developers. We review tens of thousands of apps per year and regularly disapprove noncompliant apps as part of our proactive review process. We also use tools like cease and desist letters, account suspensions, letter agreements, and civil litigation. For example, since 2006, Facebook has sent over 1,150 cease-and-desist letters to over 1,600 targets. In 2017, we took action against about 370,000 apps, ranging from imposing certain restrictions to removal of the app from the platform. Moreover, we have required parties who have procured our data without authorization to delete that data. We have invested significant resources in these efforts.

Recently, we announced a number of additional steps we're taking to address concerns raised by Kogan's app.

- **Review our platform.** We will investigate all apps that had access to large amounts of data before the platform changes we announced in 2014, and we will audit any app where we identify suspicious activity. If we identify misuses of data, we'll take immediate action, including banning the app from our platform and pursuing legal action if appropriate.

- **Tell people about data misuse.** We will tell people about apps that have misused their data. This includes building a way for people to know if their data might have been accessed via the app. Moving forward, if we remove an app, we will tell people.

- **Turn off access for unused apps.** If someone has not used an app within the last three months, we will turn off the app's access to their data.

- **Restrict Facebook Login data.** We are changing Login, so that the only data that an app can request without app review will include name, profile photo, and email address. Requesting any other data will require approval from Facebook. We will also no longer allow apps to ask for access to information like religious or political views, relationship status and details, custom friends lists, education and work history, fitness activity, book reading and music listening activity, news reading, video watch activity, and games activity. We will encourage people to manage the apps they use. We already show people what apps their accounts are connected to and allow them to control what data they've permitted those apps to use. But we're making it easier for people to see what apps they use and the information they have shared with those apps.

- **Reward people who find vulnerabilities.** We launched the Data Abuse Bounty program so that people can report to us any misuses of data by app developers.

- **Update our policies.** We have updated our terms and Data Policy to explain how we use data and how data is shared with app developers.

26. What preventative measures are being implemented so that this does not happen again?

We believe everyone deserves good privacy controls. A user owns the information they share on Facebook. This means they decide what they share and who they share it with on Facebook, and they can change their mind. We require websites and apps who use our tools to tell users they're collecting and sharing their information with us, and to get users' permission to do so.

Everyone has the right to expect strong protections for their information. We also need to do our part to help keep our community safe, in a way that's consistent with people's privacy expectations. We've recently announced several steps to give people more control over their privacy, including a new Privacy Shortcuts tool that we're rolling out now to give people information about how to control their information, including choosing who can see what they post and adding protections like two-factor authentication to their account. People can learn more about how to protect their privacy in our updated Data Policy and in our Privacy Basics feature (https://www.facebook.com/about/basics).

We are in the process of investigating every app that had access to a large amount of information before we changed our Platform in 2014. The investigation process is in full swing. We have large teams of internal and external experts working hard to investigate these apps as quickly as possible. As of early June 2018, thousands of apps have been investigated and around 200 apps have been suspended—pending a thorough investigation into whether they did in fact misuse any data. Where we find evidence that these or other apps did misuse data, we will ban them and let people know.

Facebook is generally not opposed to regulation but wants to ensure it is the right regulation. The issues facing the industry are complex, multi-faceted, and affect an important part of peoples' lives. As such, Facebook is absolutely committed to working with regulators, like Congress, to craft the right regulations. Facebook would be happy to review any proposed legislation and provide comments.

27. WHAT IS YOUR PLAN TO STOP RESALE AND THEFT OF DATA FROM FACEBOOK MEMBERS CONTACT LISTS?

We believe everyone deserves good privacy controls. A user owns the information they share on Facebook. This means they decide what they share and who they share it with on Facebook, and they can change their mind. We require websites and apps who use our tools to tell users they're collecting and sharing their information with us, and to get users' permission to do so.

Everyone has the right to expect strong protections for their information. We also need to do our part to help keep our community safe, in a way that's consistent with people's privacy expectations. We've recently announced several steps to give people more control over their privacy, including a new Privacy Shortcuts tool that we're rolling out now to give people information about how to control their information, including choosing who can see what they post and adding protections like two-factor authentication to their account. People can learn more

about how to protect their privacy in our updated Data Policy and in our Privacy Basics feature (https://www.facebook.com/about/basics).

We are in the process of investigating every app that had access to a large amount of information before we changed our Platform in 2014. The investigation process is in full swing. We have large teams of internal and external experts working hard to investigate these apps as quickly as possible. As of early June 2018, thousands of apps have been investigated and around 200 apps have been suspended—pending a thorough investigation into whether they did in fact misuse any data. Where we find evidence that these or other apps did misuse data, we will ban them and let people know.

Facebook is generally not opposed to regulation but wants to ensure it is the right regulation. The issues facing the industry are complex, multi-faceted, and affect an important part of peoples' lives. As such, Facebook is absolutely committed to working with regulators, like Congress, to craft the right regulations. Facebook would be happy to review any proposed legislation and provide comments.

28. To make a better Facebook user experience, why not give *users* access to and control over that exp?

We believe that it's important to communicate with people about the information that we collect and how people can control it. As explained in our Data Policy, we collect three basic categories of data about people:

(1) data about things people do and share (and who they connect with) on our services;

(2) data about the devices people use to access our services; and

(3) data we receive from partners, including the websites and apps that use our business tools.

We collect information about the people, Pages, accounts, hashtags, and groups users are connected to and how they interact with them across our Products, such as people a user communicates with the most or groups users are part of. We also collect contact information if they choose to upload, sync, or import it from a device (such as an address book or call log or SMS log history), which we use for things like helping them and others find people they may know.

The data we use to show ads to people depends on the data we have received from people. For people who are new to Facebook, we may have minimal data that we can use. For people who have used our services for longer, we likely have more data, but the amount of data will depend on the nature of that use and how they have used our controls. Any person can see each of the specific interests we maintain about them for advertising by visiting Ads Preferences, which lets people see what interests we use to choose ads for them—and to edit or delete these interests. We also provide more detailed information about how we use data to decide what ads to show to people in our "About Facebook Ads" page, at https://www.facebook.com/ads/about. And, we do not sell people's information to anyone, and we never will.

All users must expressly consent to Facebook's Terms and Data Policy when registering for Facebook. The Data Policy explains the kinds of information we collect, how we use this information, how we share this information, and how users can manage and delete information.

Facebook does not create profiles for people without a Facebook account, but we do receive some information from devices and browsers that may be used by non-users. For example:

- When people visit apps or websites that feature our technologies—like the Facebook Like or Comment button—our servers automatically log (i) standard browser or app records of the fact that a particular device or user visited the website or app (this connection to Facebook's servers occurs automatically when a person visits a website or app that contains our technologies, such as a Like button, and is an inherent function of Internet design); and (ii) any additional information the publisher of the app or website chooses to share with Facebook about the person's activities on that site (such as the fact that a purchase was made on the site). This is a standard feature of the Internet, and most websites and apps share this same information with multiple different third-parties whenever people visit their website or app. When the person visiting a website featuring Facebook's tools is not a registered Facebook user, Facebook does not have information identifying that individual, and it does not create profiles for this individual.

- We also may receive information about the device of a non-registered user if that user visits a part of Facebook that does not require people to log in—such as a public Facebook Page. The information we log when people visit our websites or apps is the same as described above and is the same information that any provider of an online service would receive.

- In addition, Facebook may receive some basic information about devices where Facebook apps are installed, including before people using those devices have registered for Facebook (such as when a user downloads a Facebook app, but has not yet created an account, or if the app is preloaded on a given device). This device data includes things like device model, operating system, IP address, app version and device identifiers. We use this information to provide the right version of the app, help people who want to create accounts (for example, optimizing the registration flow for the specific device), retrieving bug fixes and measuring and improving app performance. We do not use this information to build profiles about non-registered users.

29. Now that you know the high cost of your carelessness, what steps are you taking to remedy.

Facebook's policies regarding third-party usage of its platform technologies have prohibited—and continue to prohibit—third-party app developers from selling or licensing user data accessed from Facebook and from sharing any user data accessed from Facebook with any ad network, data broker or other advertising or monetization-related service. We take action on potential violations of our Platform Policies based on proactive review, external reports, and other signals. Kogan was not permitted to sell or transfer data to third-parties for the purposes he did. In doing so, Kogan and his company violated Facebook's Platform Policies.

On December 11, 2015, *The Guardian* published an article reporting that Kogan and his company, GSR, may have passed information the app had obtained from Facebook users to SCL Elections Ltd. (SCL)/Cambridge Analytica. Facebook immediately banned Kogan's app from our platform and investigated what happened and what further action Facebook should take to enforce our Platform Policies. Facebook considered the matter closed after obtaining written certifications and confirmations from Kogan, GSR, Cambridge Analytica, and SCL declaring that all such data they had obtained was accounted for and destroyed. We did not have any reason to affirmatively question the veracity of any of these certifications until March 2018, when we learned from media reporting that questions had been raised concerning the accuracy of the certifications. Facebook immediately banned Cambridge Analytica and SCL from purchasing advertisements on our services as well as removed the personal accounts of some of their officers. Moreover, while Facebook's policies in place at the time allowed us to audit apps to ensure that they were safe and did not violate its terms, we had already terminated Kogan's app's access to Facebook. Accordingly, there were no ongoing concerns about the level of data that app could access or might access in the future. With the benefit of hindsight, we wish we had notified people whose information may have been impacted. Facebook has since notified all people potentially impacted with a detailed notice at the top of their News Feed.

30. What commitments will Facebook make to allow the public full transparency and oversight of the political activities taking place on the Facebook platform?

We want our platform to be a place where people can have authentic conversations about elections and other political topics. We believe this kind of engagement promotes democracy, but we know that there are actors working to interfere with those conversations and undermine our elections. We are already taking steps to proactively prevent election interference and we are strengthening these protections going forward.

Engagement with campaigns: We want all candidates, groups, and voters to use our platform to engage in elections. We want it to be easy for people to find, follow, and contact their elected representatives—and those running to represent them. That's why, for candidates across the political spectrum, Facebook offers the same levels of support in key moments to help campaigns understand how best to use the platform. Both the Obama and Romney campaigns had access to the same tools, and no campaign received any special treatment from Facebook. Likewise, we offered identical support to both the Trump and Clinton campaigns, and had teams assigned to both. Everyone had access to the same tools, which are the same tools that every campaign is offered, and is consistent with support provided to commercial clients in the normal course of business. Facebook representatives advise political advertisers on Facebook, as they would with other, non-political managed accounts. We have a compliance team that trains our sales representatives to comply with all federal election law requirements in this area.

While no one from Facebook was assigned full-time to the Trump campaign, Facebook employees did interact with Cambridge Analytica employees. While our investigation is ongoing, our review indicates that Facebook employees did not identify any issues involving the improper use of Facebook data in the course of their interactions with Cambridge Analytica during the 2016 US Presidential campaign.

Election Integrity: In the run-up to the 2016 elections, we were focused on the kinds of cybersecurity attacks typically used by nation states, for example phishing and malware attacks. And we were too slow to spot information operations interference. Since then, we've made important changes to prevent bad actors from using misinformation to undermine the democratic process. This will never be a solved problem because we're up against determined, creative and well-funded adversaries. But we are making steady progress. Here is a list of the 10 most important changes we have made:

- **Ads transparency.** Advertising should be transparent: users should be able to see all the ads an advertiser is currently running on Facebook, Instagram, and Messenger. We are taking steps to help users assess the content they see on Facebook. For example, for ads with political content, we've created an archive that will hold ads with political content for seven years—including for information about ad impressions and spend, as well as demographic data such as age, gender, and location. People in Canada and Ireland have already been able to see all the ads that a Page is running on Facebook—and we've launched this globally. Further, advertisers will now need to confirm their ID and location before being able to run any ads with political content in the US. All ads with political content will also clearly state who paid for them. We also want to empower people to decide for themselves what to read, trust, and share. We promote news literacy and work to inform people with more context. For example, if third-party fact-checkers write articles about a news story, we show them immediately below the story in the Related Articles unit. We also notify people and Page Admins if they try to share a story, or have shared one in the past, that's been determined to be false.

- **Verification and labeling.** Every advertiser will now need confirm their ID and location before being able to run any ads with political content in the US. All ads with political content will also clearly state who paid for them.

- **Updating targeting.** We want ads on Facebook to be safe and civil. We thoroughly review the targeting criteria advertisers can use to ensure they are consistent with our principles. As a result, we removed nearly one-third of the targeting segments used by the IRA. We continue to allow some criteria that people may find controversial. But we do see businesses marketing things like historical books, documentaries or television shows using them in legitimate ways.

- **Better technology.** Over the past year, we've gotten increasingly better at finding and disabling fake accounts. We now block millions of fake accounts each day as people try to create them—and before they've done any harm. This is thanks to improvements in machine learning and artificial intelligence, which can proactively identify suspicious behavior at a scale that was not possible before—without needing to look at the content itself.

- **Action to tackle fake news.** We are working hard to stop the spread of false news. We work with third party fact checking organizations to limit the spread of

articles rated false. To reduce the spread of false news, we remove fake accounts and disrupt economic incentives for traffickers of misinformation. We also use various signals, including feedback from our community, to identify potential false news. In countries where we have partnerships with independent third-party fact-checkers, stories rated as false by those fact-checkers are shown lower in News Feed. If Pages or domains repeatedly create or share misinformation, we significantly reduce their distribution and remove their advertising rights. We also want to empower people to decide for themselves what to read, trust, and share. We promote news literacy and work to inform people with more context. For example, if third-party fact-checkers write articles about a news story, we show them immediately below the story in the Related Articles unit. We also notify people and Page Admins if they try to share a story, or have shared one in the past, that's been determined to be false. In addition to our own efforts, we're learning from academics, scaling our partnerships with third-party fact-checkers and talking to other organizations about how we can work together.

- **Significant investments in security.** We're doubling the number of people working on safety and security from 10,000 last year to over 20,000 this year. We expect these investments to impact our profitability. But the safety of people using Facebook needs to come before profit.

- **Industry collaboration.** In April, we joined 34 global tech and security companies in signing a TechAccord pact to help improve security for everyone.

- **Intelligence sharing with government.** In the 2017 German elections, we worked closely with the authorities there, including the Federal Office for Information Security (BSI). This gave them a dedicated reporting channel for security issues related to the federal elections.

- Tracking 40+ elections. In recent months, we've started to deploy new tools and teams to proactively identify threats in the run-up to specific elections. We first tested this effort during the Alabama Senate election, and plan to continue these efforts for elections around the globe, including the US midterms. Last year we used public service announcements to help inform people about fake news in 21 separate countries, including in advance of French, Kenyan, and German elections.

- Action against the Russia-based IRA. In April, we removed 70 Facebook and 65 Instagram accounts—as well as 138 Facebook Pages—controlled by the IRA primarily targeted either at people living in Russia or Russian-speakers around the world including from neighboring countries like Azerbaijan, Uzbekistan, and Ukraine. The IRA has repeatedly used complex networks of inauthentic accounts to deceive and manipulate people in the US, Europe, and Russia—and we don't want them on Facebook anywhere in the world. We are taking steps to enhance trust in the authenticity of activity on our platform, including increasing ads transparency, implementing a more robust ads review process, imposing tighter content restrictions, and exploring how to add additional authenticity safeguards.

We also have improved information sharing about these issues among our industry partners.

31. What steps are you taking to retrieve and delete the information that has already been scraped?

Facebook's policies regarding third-party usage of its platform technologies have prohibited—and continue to prohibit—third-party app developers from selling or licensing user data obtained from Facebook and from sharing any user data obtained from Facebook with any ad network, data broker or other advertising or monetization-related service.

We use a variety of tools to enforce Facebook policies against violating parties, including developers. We review tens of thousands of apps per year and regularly disapprove noncompliant apps as part of our proactive review process. We also use tools like cease and desist letters, account suspensions, letter agreements, and civil litigation. For example, since 2006, Facebook has sent over 1,150 cease-and-desist letters to over 1,600 targets. In 2017, we took action against about 370,000 apps, ranging from imposing certain restrictions to removal of the app from the platform. Moreover, we have required parties who have procured our data without authorization to delete that data. We have invested significant resources in these efforts.

Recently, we announced a number of additional steps we're taking to address concerns raised by Kogan's app.

- **Review our platform.** We will investigate all apps that had access to large amounts of data before the platform changes we announced in 2014, and we will audit any app where we identify suspicious activity. If we identify misuses of data, we'll take immediate action, including banning the app from our platform and pursuing legal action if appropriate.

- **Tell people about data misuse.** We will tell people about apps that have misused their data. This includes building a way for people to know if their data might have been accessed via the app. Moving forward, if we remove an app, we will tell people.

- **Turn off access for unused apps.** If someone has not used an app within the last three months, we will turn off the app's access to their data.

- **Restrict Facebook Login data.** We are changing Login, so that the only data that an app can request without app review will include name, profile photo, and email address. Requesting any other data will require approval from Facebook. We will also no longer allow apps to ask for access to information like religious or political views, relationship status and details, custom friends lists, education and work history, fitness activity, book reading and music listening activity, news reading, video watch activity, and games activity. We will encourage people to manage the apps they use. We already show people what apps their accounts are connected to and allow them to control what data they've permitted those apps to use. But we're making it easier for people to see what apps they use and the information they have shared with those apps.

- **Reward people who find vulnerabilities.** We launched the Data Abuse Bounty program so that people can report to us any misuses of data by app developers.

- **Update our policies.** We have updated our terms and Data Policy to explain how we use data and how data is shared with app developers.

32. Can we be sure it won't happen again?

Facebook's policies regarding third-party usage of its platform technologies have prohibited—and continue to prohibit—third-party app developers from selling or licensing user data obtained from Facebook and from sharing any user data obtained from Facebook with any ad network, data broker or other advertising or monetization-related service.

We use a variety of tools to enforce Facebook policies against violating parties, including developers. We review tens of thousands of apps per year and regularly disapprove noncompliant apps as part of our proactive review process. We also use tools like cease and desist letters, account suspensions, letter agreements, and civil litigation. For example, since 2006, Facebook has sent over 1,150 cease-and-desist letters to over 1,600 targets. In 2017, we took action against about 370,000 apps, ranging from imposing certain restrictions to removal of the app from the platform. Moreover, we have required parties who have procured our data without authorization to delete that data. We have invested significant resources in these efforts.

Recently, we announced a number of additional steps we're taking to address concerns raised by Kogan's app.

- **Review our platform.** We will investigate all apps that had access to large amounts of data before the platform changes we announced in 2014, and we will audit any app where we identify suspicious activity. If we identify misuses of data, we'll take immediate action, including banning the app from our platform and pursuing legal action if appropriate.

- **Tell people about data misuse.** We will tell people about apps that have misused their data. This includes building a way for people to know if their data might have been accessed via the app. Moving forward, if we remove an app, we will tell people.

- **Turn off access for unused apps.** If someone has not used an app within the last three months, we will turn off the app's access to their data.

- **Restrict Facebook Login data.** We are changing Login, so that the only data that an app can request without app review will include name, profile photo, and email address. Requesting any other data will require approval from Facebook. We will also no longer allow apps to ask for access to information like religious or political views, relationship status and details, custom friends lists, education and work history, fitness activity, book reading and music listening activity, news reading, video watch activity, and games activity. We will encourage people to manage the apps they use. We already show people what apps their accounts are connected to and allow them to control what data they've permitted those apps to use. But we're making it easier for

people to see what apps they use and the information they have shared with those apps.

- **Reward people who find vulnerabilities.** We launched the Data Abuse Bounty program so that people can report to us any misuses of data by app developers.

- **Update our policies.** We have updated our terms and Data Policy to explain how we use data and how data is shared with app developers.

33. What steps have you taken to assure that this kind of data stealing does not happen in the future?

We believe everyone deserves good privacy controls. A user owns the information they share on Facebook. This means they decide what they share and who they share it with on Facebook, and they can change their mind. We require websites and apps who use our tools to tell users they're collecting and sharing their information with us, and to get users' permission to do so.

Everyone has the right to expect strong protections for their information. We also need to do our part to help keep our community safe, in a way that's consistent with people's privacy expectations. We've recently announced several steps to give people more control over their privacy, including a new Privacy Shortcuts tool that we're rolling out now to give people information about how to control their information, including choosing who can see what they post and adding protections like two-factor authentication to their account. People can learn more about how to protect their privacy in our updated Data Policy and in our Privacy Basics feature (https://www.facebook.com/about/basics).

We are in the process of investigating every app that had access to a large amount of information before we changed our Platform in 2014. The investigation process is in full swing. We have large teams of internal and external experts working hard to investigate these apps as quickly as possible. As of early June 2018, thousands of apps have been investigated and around 200 apps have been suspended—pending a thorough investigation into whether they did in fact misuse any data. Where we find evidence that these or other apps did misuse data, we will ban them and let people know.

Facebook is generally not opposed to regulation but wants to ensure it is the right regulation. The issues facing the industry are complex, multi-faceted, and affect an important part of peoples' lives. As such, Facebook is absolutely committed to working with regulators, like Congress, to craft the right regulations. Facebook would be happy to review any proposed legislation and provide comments.

34. What other vulnerabilities is Facebook addressing?

We believe everyone deserves good privacy controls. A user owns the information they share on Facebook. This means they decide what they share and who they share it with on Facebook, and they can change their mind. We require websites and apps who use our tools to tell users they're collecting and sharing their information with us, and to get users' permission to do so.

Everyone has the right to expect strong protections for their information. We also need to do our part to help keep our community safe, in a way that's consistent with people's privacy expectations. We've recently announced several steps to give people more control over their privacy, including a new Privacy Shortcuts tool that we're rolling out now to give people information about how to control their information, including choosing who can see what they post and adding protections like two-factor authentication to their account. People can learn more about how to protect their privacy in our updated Data Policy and in our Privacy Basics feature (https://www.facebook.com/about/basics).

We are in the process of investigating every app that had access to a large amount of information before we changed our Platform in 2014. The investigation process is in full swing. We have large teams of internal and external experts working hard to investigate these apps as quickly as possible. As of early June 2018, thousands of apps have been investigated and around 200 apps have been suspended—pending a thorough investigation into whether they did in fact misuse any data. Where we find evidence that these or other apps did misuse data, we will ban them and let people know.

Facebook is generally not opposed to regulation but wants to ensure it is the right regulation. The issues facing the industry are complex, multi-faceted, and affect an important part of peoples' lives. As such, Facebook is absolutely committed to working with regulators, like Congress, to craft the right regulations. Facebook would be happy to review any proposed legislation and provide comments.

35. Does he plan to notify all the affected consumers and let them know EXACTLY the data breached?

Facebook's policies regarding third-party usage of its platform technologies have prohibited—and continue to prohibit—third-party app developers from selling or licensing user data accessed from Facebook and from sharing any user data accessed from Facebook with any ad network, data broker or other advertising or monetization-related service. We take action on potential violations of our Platform Policies based on proactive review, external reports, and other signals. Kogan was not permitted to sell or transfer data to third-parties for the purposes he did. In doing so, Kogan and his company violated Facebook's Platform Policies.

On December 11, 2015, *The Guardian* published an article reporting that Kogan and his company, GSR, may have passed information the app had obtained from Facebook users to SCL Elections Ltd. (SCL)/Cambridge Analytica. Facebook immediately banned Kogan's app from our platform and investigated what happened and what further action Facebook should take to enforce our Platform Policies. Facebook considered the matter closed after obtaining written certifications and confirmations from Kogan, GSR, Cambridge Analytica, and SCL declaring that all such data they had obtained was accounted for and destroyed. We did not have any reason to affirmatively question the veracity of any of these certifications until March 2018, when we learned from media reporting that questions had been raised concerning the accuracy of the certifications. Facebook immediately banned Cambridge Analytica and SCL from purchasing advertisements on our services as well as removed the personal accounts of some of their officers. Moreover, while Facebook's policies in place at the time allowed us to audit apps to ensure that they were safe and did not violate its terms, we had already terminated Kogan's app's

access to Facebook. Accordingly, there were no ongoing concerns about the level of data that app could access or might access in the future. With the benefit of hindsight, we wish we had notified people whose information may have been impacted. Facebook has since notified all people potentially impacted with a detailed notice at the top of their News Feed.

36. What will you do to prevent this from happening again?

Facebook's policies regarding third-party usage of its platform technologies have prohibited—and continue to prohibit—third-party app developers from selling or licensing user data obtained from Facebook and from sharing any user data obtained from Facebook with any ad network, data broker or other advertising or monetization-related service.

We use a variety of tools to enforce Facebook policies against violating parties, including developers. We review tens of thousands of apps per year and regularly disapprove noncompliant apps as part of our proactive review process. We also use tools like cease and desist letters, account suspensions, letter agreements, and civil litigation. For example, since 2006, Facebook has sent over 1,150 cease-and-desist letters to over 1,600 targets. In 2017, we took action against about 370,000 apps, ranging from imposing certain restrictions to removal of the app from the platform. Moreover, we have required parties who have procured our data without authorization to delete that data. We have invested significant resources in these efforts.

Recently, we announced a number of additional steps we're taking to address concerns raised by Kogan's app.

- **Review our platform.** We will investigate all apps that had access to large amounts of data before the platform changes we announced in 2014, and we will audit any app where we identify suspicious activity. If we identify misuses of data, we'll take immediate action, including banning the app from our platform and pursuing legal action if appropriate.

- **Tell people about data misuse.** We will tell people about apps that have misused their data. This includes building a way for people to know if their data might have been accessed via the app. Moving forward, if we remove an app, we will tell people.

- **Turn off access for unused apps.** If someone has not used an app within the last three months, we will turn off the app's access to their data.

- **Restrict Facebook Login data.** We are changing Login, so that the only data that an app can request without app review will include name, profile photo, and email address. Requesting any other data will require approval from Facebook. We will also no longer allow apps to ask for access to information like religious or political views, relationship status and details, custom friends lists, education and work history, fitness activity, book reading and music listening activity, news reading, video watch activity, and games activity. We will encourage people to manage the apps they use. We already show people what apps their accounts are connected to and allow them to control what data they've permitted those apps to use. But we're making it easier for

people to see what apps they use and the information they have shared with those apps.

- **Reward people who find vulnerabilities.** We launched the Data Abuse Bounty program so that people can report to us any misuses of data by app developers.

- **Update our policies.** We have updated our terms and Data Policy to explain how we use data and how data is shared with app developers.

37. What steps are you going to take to earn our trust?

We believe everyone deserves good privacy controls. A user owns the information they share on Facebook. This means they decide what they share and who they share it with on Facebook, and they can change their mind. We require websites and apps who use our tools to tell users they're collecting and sharing their information with us, and to get users' permission to do so.

Everyone has the right to expect strong protections for their information. We also need to do our part to help keep our community safe, in a way that's consistent with people's privacy expectations. We've recently announced several steps to give people more control over their privacy, including a new Privacy Shortcuts tool that we're rolling out now to give people information about how to control their information, including choosing who can see what they post and adding protections like two-factor authentication to their account. People can learn more about how to protect their privacy in our updated Data Policy and in our Privacy Basics feature (https://www.facebook.com/about/basics).

We are in the process of investigating every app that had access to a large amount of information before we changed our Platform in 2014. The investigation process is in full swing. We have large teams of internal and external experts working hard to investigate these apps as quickly as possible. As of early June 2018, thousands of apps have been investigated and around 200 apps have been suspended—pending a thorough investigation into whether they did in fact misuse any data. Where we find evidence that these or other apps did misuse data, we will ban them and let people know.

Facebook is generally not opposed to regulation but wants to ensure it is the right regulation. The issues facing the industry are complex, multi-faceted, and affect an important part of peoples' lives. As such, Facebook is absolutely committed to working with regulators, like Congress, to craft the right regulations. Facebook would be happy to review any proposed legislation and provide comments.

38. What changes will be taken to insure transparency in advertising sources?

To build a secure product with extensive infrastructure that connects people wherever they live or whatever their income level, we need to make sure everyone can afford it. Advertising lets us keep Facebook free, which ensures it remains affordable for everyone. We also believe the ads you see across the Facebook family of apps and services should be useful and relevant to you. Users can't opt out of seeing ads altogether because selling ads is what keeps Facebook free, but they do have different options to control how their data can and can't

be used to show them ads. They're all found in ad preferences, which allows users to turn off the use of all data collected from partners off Facebook to target ads. Users can also decide which of their profile fields they want used for ad targeting in the Information section under "About you." Users can remove themselves from interests under "Your interests" and categories under "Your categories." And, we do not sell people's information to anyone, and we never will.

Facebook is committed to transparency for all ads, including ads with political content. Facebook believes that people should be able to easily understand why they are seeing ads, who paid for them, and what other ads those advertisers are running. As such, Facebook only allows authorized advertisers to run ads about elections or issues that are being debated across the country. In order to be authorized by Facebook, advertisers will need to confirm their identity and location. Furthermore, all political and issue ads will include a disclosure which reads: "Paid for by," and when users click on this disclosure they will be able to see details about the advertiser. Users will also be able to see an explanation of why they saw the particular ad. This is similar to the disclosure included on political TV advertisements. We just launched globally View Active Ads, a feature that will enable anyone to see all of the ads an advertiser is currently running by visiting the advertiser's Facebook Page.

39. Americans do not yet fully understand the high cost of free. What are you willing to do at Facebook?

As discussed with your staff, this question is not germane to the hearing.

40. Despite its best intentions, Facebook has continued to make decisions about privacy that help Facebook itself at the expense of users, from features like Beacon to the latest scandal about oversharing data with third-party apps. It seems like each time a problem is fixed, a new one appears. Whatever process is in place, it doesn't seem to be working. So my question is, what fundamental changes is Facebook making to prevent these sort of user-hostile decisions from being made in the future?

We believe everyone deserves good privacy controls. A user owns the information they share on Facebook. This means they decide what they share and who they share it with on Facebook, and they can change their mind. We require websites and apps who use our tools to tell users they're collecting and sharing their information with us, and to get users' permission to do so.

Everyone has the right to expect strong protections for their information. We also need to do our part to help keep our community safe, in a way that's consistent with people's privacy expectations. We've recently announced several steps to give people more control over their privacy, including a new Privacy Shortcuts tool that we're rolling out now to give people information about how to control their information, including choosing who can see what they post and adding protections like two-factor authentication to their account. People can learn more about how to protect their privacy in our updated Data Policy and in our Privacy Basics feature (https://www.facebook.com/about/basics).

We are in the process of investigating every app that had access to a large amount of information before we changed our Platform in 2014. The investigation process is in full swing.

We have large teams of internal and external experts working hard to investigate these apps as quickly as possible. As of early June 2018, thousands of apps have been investigated and around 200 apps have been suspended—pending a thorough investigation into whether they did in fact misuse any data. Where we find evidence that these or other apps did misuse data, we will ban them and let people know.

Facebook is generally not opposed to regulation but wants to ensure it is the right regulation. The issues facing the industry are complex, multi-faceted, and affect an important part of peoples' lives. As such, Facebook is absolutely committed to working with regulators, like Congress, to craft the right regulations. Facebook would be happy to review any proposed legislation and provide comments.

41. What controls do you plan to put in place to protect privacy and prevent misuse of data?

We believe everyone deserves good privacy controls. A user owns the information they share on Facebook. This means they decide what they share and who they share it with on Facebook, and they can change their mind. We require websites and apps who use our tools to tell users they're collecting and sharing their information with us, and to get users' permission to do so.

Everyone has the right to expect strong protections for their information. We also need to do our part to help keep our community safe, in a way that's consistent with people's privacy expectations. We've recently announced several steps to give people more control over their privacy, including a new Privacy Shortcuts tool that we're rolling out now to give people information about how to control their information, including choosing who can see what they post and adding protections like two-factor authentication to their account. People can learn more about how to protect their privacy in our updated Data Policy and in our Privacy Basics feature (https://www.facebook.com/about/basics).

We are in the process of investigating every app that had access to a large amount of information before we changed our Platform in 2014. The investigation process is in full swing. We have large teams of internal and external experts working hard to investigate these apps as quickly as possible. As of early June 2018, thousands of apps have been investigated and around 200 apps have been suspended—pending a thorough investigation into whether they did in fact misuse any data. Where we find evidence that these or other apps did misuse data, we will ban them and let people know.

Facebook is generally not opposed to regulation but wants to ensure it is the right regulation. The issues facing the industry are complex, multi-faceted, and affect an important part of peoples' lives. As such, Facebook is absolutely committed to working with regulators, like Congress, to craft the right regulations. Facebook would be happy to review any proposed legislation and provide comments.

42. Are rumors true that FB's considering charging users to ensure protection of privacy?

We believe everyone deserves good privacy controls. A user owns the information they share on Facebook. This means they decide what they share and who they share it with on Facebook, and they can change their mind. We require websites and apps who use our tools to tell users they're collecting and sharing their information with us, and to get users' permission to do so.

Everyone has the right to expect strong protections for their information. We also need to do our part to help keep our community safe, in a way that's consistent with people's privacy expectations. We've recently announced several steps to give people more control over their privacy, including a new Privacy Shortcuts tool that we're rolling out now to give people information about how to control their information, including choosing who can see what they post and adding protections like two-factor authentication to their account. People can learn more about how to protect their privacy in our updated Data Policy and in our Privacy Basics feature (https://www.facebook.com/about/basics).

We are in the process of investigating every app that had access to a large amount of information before we changed our Platform in 2014. The investigation process is in full swing. We have large teams of internal and external experts working hard to investigate these apps as quickly as possible. As of early June 2018, thousands of apps have been investigated and around 200 apps have been suspended—pending a thorough investigation into whether they did in fact misuse any data. Where we find evidence that these or other apps did misuse data, we will ban them and let people know.

Facebook is generally not opposed to regulation but wants to ensure it is the right regulation. The issues facing the industry are complex, multi-faceted, and affect an important part of peoples' lives. As such, Facebook is absolutely committed to working with regulators, like Congress, to craft the right regulations. Facebook would be happy to review any proposed legislation and provide comments.

43. What specific steps are you taking to ensure that all Facebook users' data is secure and protected?

We believe everyone deserves good privacy controls. A user owns the information they share on Facebook. This means they decide what they share and who they share it with on Facebook, and they can change their mind. We require websites and apps who use our tools to tell users they're collecting and sharing their information with us, and to get users' permission to do so.

Everyone has the right to expect strong protections for their information. We also need to do our part to help keep our community safe, in a way that's consistent with people's privacy expectations. We've recently announced several steps to give people more control over their privacy, including a new Privacy Shortcuts tool that we're rolling out now to give people information about how to control their information, including choosing who can see what they post and adding protections like two-factor authentication to their account. People can learn more about how to protect their privacy in our updated Data Policy and in our Privacy Basics feature (https://www.facebook.com/about/basics).

We are in the process of investigating every app that had access to a large amount of information before we changed our Platform in 2014. The investigation process is in full swing. We have large teams of internal and external experts working hard to investigate these apps as quickly as possible. As of early June 2018, thousands of apps have been investigated and around 200 apps have been suspended—pending a thorough investigation into whether they did in fact misuse any data. Where we find evidence that these or other apps did misuse data, we will ban them and let people know.

Facebook is generally not opposed to regulation but wants to ensure it is the right regulation. The issues facing the industry are complex, multi-faceted, and affect an important part of peoples' lives. As such, Facebook is absolutely committed to working with regulators, like Congress, to craft the right regulations. Facebook would be happy to review any proposed legislation and provide comments.

44. What will Facebook do to prevent this security breach from happening again?

We believe everyone deserves good privacy controls. A user owns the information they share on Facebook. This means they decide what they share and who they share it with on Facebook, and they can change their mind. We require websites and apps who use our tools to tell users they're collecting and sharing their information with us, and to get users' permission to do so.

Everyone has the right to expect strong protections for their information. We also need to do our part to help keep our community safe, in a way that's consistent with people's privacy expectations. We've recently announced several steps to give people more control over their privacy, including a new Privacy Shortcuts tool that we're rolling out now to give people information about how to control their information, including choosing who can see what they post and adding protections like two-factor authentication to their account. People can learn more about how to protect their privacy in our updated Data Policy and in our Privacy Basics feature (https://www.facebook.com/about/basics).

We are in the process of investigating every app that had access to a large amount of information before we changed our Platform in 2014. The investigation process is in full swing. We have large teams of internal and external experts working hard to investigate these apps as quickly as possible. As of early June 2018, thousands of apps have been investigated and around 200 apps have been suspended—pending a thorough investigation into whether they did in fact misuse any data. Where we find evidence that these or other apps did misuse data, we will ban them and let people know.

Facebook is generally not opposed to regulation but wants to ensure it is the right regulation. The issues facing the industry are complex, multi-faceted, and affect an important part of peoples' lives. As such, Facebook is absolutely committed to working with regulators, like Congress, to craft the right regulations. Facebook would be happy to review any proposed legislation and provide comments.

45. How will you make amends for illegally distributing private information of my constituents?

We believe everyone deserves good privacy controls. A user owns the information they share on Facebook. This means they decide what they share and who they share it with on Facebook, and they can change their mind. We require websites and apps who use our tools to tell users they're collecting and sharing their information with us, and to get users' permission to do so.

Everyone has the right to expect strong protections for their information. We also need to do our part to help keep our community safe, in a way that's consistent with people's privacy expectations. We've recently announced several steps to give people more control over their privacy, including a new Privacy Shortcuts tool that we're rolling out now to give people information about how to control their information, including choosing who can see what they post and adding protections like two-factor authentication to their account. People can learn more about how to protect their privacy in our updated Data Policy and in our Privacy Basics feature (https://www.facebook.com/about/basics).

We are in the process of investigating every app that had access to a large amount of information before we changed our Platform in 2014. The investigation process is in full swing. We have large teams of internal and external experts working hard to investigate these apps as quickly as possible. As of early June 2018, thousands of apps have been investigated and around 200 apps have been suspended—pending a thorough investigation into whether they did in fact misuse any data. Where we find evidence that these or other apps did misuse data, we will ban them and let people know.

Facebook is generally not opposed to regulation but wants to ensure it is the right regulation. The issues facing the industry are complex, multi-faceted, and affect an important part of peoples' lives. As such, Facebook is absolutely committed to working with regulators, like Congress, to craft the right regulations. Facebook would be happy to review any proposed legislation and provide comments.

46. Can hacking be totally prevented in the future?

For years, we had been aware of other types of activity that appeared to come from Russian sources—largely traditional security threats such as attacking people's accounts or using social media platforms to spread stolen information. What we saw early in the 2016 campaign cycle followed this pattern. Our security team that focuses on threat intelligence—which investigates advanced security threats as part of our overall information security organization—was, from the outset, alert to the possibility of Russian activity. In several instances before November 8, 2016, this team detected and mitigated threats from actors with ties to Russia and reported them to US law enforcement officials. This included activity from a cluster of accounts we had assessed to belong to a group (APT28) that the US government has publicly linked to Russian military intelligence services. This activity, which was aimed at employees of major US political parties, fell into the normal categories of offensive cyber activities we monitor for. We warned the targets who were at highest risk, and were later in contact with law enforcement authorities about this activity.

Later in the summer we also started to see a new kind of behavior from APT28-related accounts—namely, the creation of fake personas that were then used to seed stolen information

to journalists. These fake personas were organized under the banner of an organization that called itself DC Leaks. This activity violated our policies, and we removed the DC Leaks accounts.

Facebook learned from press accounts and statements by congressional leaders that Russian actors might have tried to interfere in the 2016 election by exploiting Facebook's ad tools. This is not something we had seen before, and so we started an investigation. We found that fake accounts associated with the IRA tried to influence the election.

This will never be a solved problem because we're up against determined, creative and well-funded adversaries. But we are making steady progress in preventing bad actors from using misinformation to undermine the democratic process, such as: increased ad transparency, advertiser verification and labeling, updating targeting criteria, better technological efforts to find and disable fake accounts, third-party fact checking to stop the spread of false news, doubling the number of people working on safety and security, greater industry collaboration, increased information sharing and reporting channels, proactive identification of election threats, and specific action against the Russia-based IRA.

We will continue to work with the government, and across the tech industry and civil society, to address this important national security matter so that we can do our part to prevent similar abuse from happening again.

47. What concrete steps can you show the American public that you will put social responsibility above $?

We believe everyone deserves good privacy controls. A user owns the information they share on Facebook. This means they decide what they share and who they share it with on Facebook, and they can change their mind. We require websites and apps who use our tools to tell users they're collecting and sharing their information with us, and to get users' permission to do so.

Everyone has the right to expect strong protections for their information. We also need to do our part to help keep our community safe, in a way that's consistent with people's privacy expectations. We've recently announced several steps to give people more control over their privacy, including a new Privacy Shortcuts tool that we're rolling out now to give people information about how to control their information, including choosing who can see what they post and adding protections like two-factor authentication to their account. People can learn more about how to protect their privacy in our updated Data Policy and in our Privacy Basics feature (https://www.facebook.com/about/basics).

We are in the process of investigating every app that had access to a large amount of information before we changed our Platform in 2014. The investigation process is in full swing. We have large teams of internal and external experts working hard to investigate these apps as quickly as possible. As of early June 2018, thousands of apps have been investigated and around 200 apps have been suspended—pending a thorough investigation into whether they did in fact misuse any data. Where we find evidence that these or other apps did misuse data, we will ban them and let people know.

Facebook is generally not opposed to regulation but wants to ensure it is the right regulation. The issues facing the industry are complex, multi-faceted, and affect an important part of peoples' lives. As such, Facebook is absolutely committed to working with regulators, like Congress, to craft the right regulations. Facebook would be happy to review any proposed legislation and provide comments.

48. What do you plan to do in the future to prevent a repeat and guard our privacy?

We believe everyone deserves good privacy controls. A user owns the information they share on Facebook. This means they decide what they share and who they share it with on Facebook, and they can change their mind. We require websites and apps who use our tools to tell users they're collecting and sharing their information with us, and to get users' permission to do so.

Everyone has the right to expect strong protections for their information. We also need to do our part to help keep our community safe, in a way that's consistent with people's privacy expectations. We've recently announced several steps to give people more control over their privacy, including a new Privacy Shortcuts tool that we're rolling out now to give people information about how to control their information, including choosing who can see what they post and adding protections like two-factor authentication to their account. People can learn more about how to protect their privacy in our updated Data Policy and in our Privacy Basics feature (https://www.facebook.com/about/basics).

We are in the process of investigating every app that had access to a large amount of information before we changed our Platform in 2014. The investigation process is in full swing. We have large teams of internal and external experts working hard to investigate these apps as quickly as possible. As of early June 2018, thousands of apps have been investigated and around 200 apps have been suspended—pending a thorough investigation into whether they did in fact misuse any data. Where we find evidence that these or other apps did misuse data, we will ban them and let people know.

Facebook is generally not opposed to regulation but wants to ensure it is the right regulation. The issues facing the industry are complex, multi-faceted, and affect an important part of peoples' lives. As such, Facebook is absolutely committed to working with regulators, like Congress, to craft the right regulations. Facebook would be happy to review any proposed legislation and provide comments.

49. Users want the ability to limit the data about them that is collected. Can you commit to that?

We believe everyone deserves good privacy controls. A user owns the information they share on Facebook. This means they decide what they share and who they share it with on Facebook, and they can change their mind. We require websites and apps who use our tools to tell users they're collecting and sharing their information with us, and to get users' permission to do so.

Everyone has the right to expect strong protections for their information. We also need to do our part to help keep our community safe, in a way that's consistent with people's privacy

expectations. We've recently announced several steps to give people more control over their privacy, including a new Privacy Shortcuts tool that we're rolling out now to give people information about how to control their information, including choosing who can see what they post and adding protections like two-factor authentication to their account. People can learn more about how to protect their privacy in our updated Data Policy and in our Privacy Basics feature (https://www.facebook.com/about/basics).

We are in the process of investigating every app that had access to a large amount of information before we changed our Platform in 2014. The investigation process is in full swing. We have large teams of internal and external experts working hard to investigate these apps as quickly as possible. As of early June 2018, thousands of apps have been investigated and around 200 apps have been suspended—pending a thorough investigation into whether they did in fact misuse any data. Where we find evidence that these or other apps did misuse data, we will ban them and let people know.

Facebook is generally not opposed to regulation but wants to ensure it is the right regulation. The issues facing the industry are complex, multi-faceted, and affect an important part of peoples' lives. As such, Facebook is absolutely committed to working with regulators, like Congress, to craft the right regulations. Facebook would be happy to review any proposed legislation and provide comments.

50. Moving forward what will be done to prevent future slips and any steps to recoup?

Facebook's policies regarding third-party usage of its platform technologies have prohibited—and continue to prohibit—third-party app developers from selling or licensing user data obtained from Facebook and from sharing any user data obtained from Facebook with any ad network, data broker or other advertising or monetization-related service.

We use a variety of tools to enforce Facebook policies against violating parties, including developers. We review tens of thousands of apps per year and regularly disapprove noncompliant apps as part of our proactive review process. We also use tools like cease and desist letters, account suspensions, letter agreements, and civil litigation. For example, since 2006, Facebook has sent over 1,150 cease-and-desist letters to over 1,600 targets. In 2017, we took action against about 370,000 apps, ranging from imposing certain restrictions to removal of the app from the platform. Moreover, we have required parties who have procured our data without authorization to delete that data. We have invested significant resources in these efforts.

Recently, we announced a number of additional steps we're taking to address concerns raised by Kogan's app.

- **Review our platform.** We will investigate all apps that had access to large amounts of data before the platform changes we announced in 2014, and we will audit any app where we identify suspicious activity. If we identify misuses of data, we'll take immediate action, including banning the app from our platform and pursuing legal action if appropriate.

- **Tell people about data misuse.** We will tell people about apps that have misused their data. This includes building a way for people to know if their data might have been accessed via the app. Moving forward, if we remove an app, we will tell people.

- **Turn off access for unused apps.** If someone has not used an app within the last three months, we will turn off the app's access to their data.

- **Restrict Facebook Login data.** We are changing Login, so that the only data that an app can request without app review will include name, profile photo, and email address. Requesting any other data will require approval from Facebook. We will also no longer allow apps to ask for access to information like religious or political views, relationship status and details, custom friends lists, education and work history, fitness activity, book reading and music listening activity, news reading, video watch activity, and games activity. We will encourage people to manage the apps they use. We already show people what apps their accounts are connected to and allow them to control what data they've permitted those apps to use. But we're making it easier for people to see what apps they use and the information they have shared with those apps.

- **Reward people who find vulnerabilities.** We launched the Data Abuse Bounty program so that people can report to us any misuses of data by app developers.

- **Update our policies.** We have updated our terms and Data Policy to explain how we use data and how data is shared with app developers.

51. Please tell us what you have done, rather than are going to do to address these problems.

We believe everyone deserves good privacy controls. A user owns the information they share on Facebook. This means they decide what they share and who they share it with on Facebook, and they can change their mind. We require websites and apps who use our tools to tell users they're collecting and sharing their information with us, and to get users' permission to do so.

Everyone has the right to expect strong protections for their information. We also need to do our part to help keep our community safe, in a way that's consistent with people's privacy expectations. We've recently announced several steps to give people more control over their privacy, including a new Privacy Shortcuts tool that we're rolling out now to give people information about how to control their information, including choosing who can see what they post and adding protections like two-factor authentication to their account. People can learn more about how to protect their privacy in our updated Data Policy and in our Privacy Basics feature (https://www.facebook.com/about/basics).

We are in the process of investigating every app that had access to a large amount of information before we changed our Platform in 2014. The investigation process is in full swing. We have large teams of internal and external experts working hard to investigate these apps as quickly as possible. As of early June 2018, thousands of apps have been investigated and around

200 apps have been suspended—pending a thorough investigation into whether they did in fact misuse any data. Where we find evidence that these or other apps did misuse data, we will ban them and let people know.

Facebook is generally not opposed to regulation but wants to ensure it is the right regulation. The issues facing the industry are complex, multi-faceted, and affect an important part of peoples' lives. As such, Facebook is absolutely committed to working with regulators, like Congress, to craft the right regulations. Facebook would be happy to review any proposed legislation and provide comments.

52. What steps can and will you take to insure our privacy in the future?

We believe everyone deserves good privacy controls. A user owns the information they share on Facebook. This means they decide what they share and who they share it with on Facebook, and they can change their mind. We require websites and apps who use our tools to tell users they're collecting and sharing their information with us, and to get users' permission to do so.

Everyone has the right to expect strong protections for their information. We also need to do our part to help keep our community safe, in a way that's consistent with people's privacy expectations. We've recently announced several steps to give people more control over their privacy, including a new Privacy Shortcuts tool that we're rolling out now to give people information about how to control their information, including choosing who can see what they post and adding protections like two-factor authentication to their account. People can learn more about how to protect their privacy in our updated Data Policy and in our Privacy Basics feature (https://www.facebook.com/about/basics).

We are in the process of investigating every app that had access to a large amount of information before we changed our Platform in 2014. The investigation process is in full swing. We have large teams of internal and external experts working hard to investigate these apps as quickly as possible. As of early June 2018, thousands of apps have been investigated and around 200 apps have been suspended—pending a thorough investigation into whether they did in fact misuse any data. Where we find evidence that these or other apps did misuse data, we will ban them and let people know.

Facebook is generally not opposed to regulation but wants to ensure it is the right regulation. The issues facing the industry are complex, multi-faceted, and affect an important part of peoples' lives. As such, Facebook is absolutely committed to working with regulators, like Congress, to craft the right regulations. Facebook would be happy to review any proposed legislation and provide comments.

53. How will you keep my information safe going forward? What will you do to fix illegally obtained info?

We believe everyone deserves good privacy controls. A user owns the information they share on Facebook. This means they decide what they share and who they share it with on Facebook, and they can change their mind. We require websites and apps who use our tools to

tell users they're collecting and sharing their information with us, and to get users' permission to do so.

Everyone has the right to expect strong protections for their information. We also need to do our part to help keep our community safe, in a way that's consistent with people's privacy expectations. We've recently announced several steps to give people more control over their privacy, including a new Privacy Shortcuts tool that we're rolling out now to give people information about how to control their information, including choosing who can see what they post and adding protections like two-factor authentication to their account. People can learn more about how to protect their privacy in our updated Data Policy and in our Privacy Basics feature (https://www.facebook.com/about/basics).

We are in the process of investigating every app that had access to a large amount of information before we changed our Platform in 2014. The investigation process is in full swing. We have large teams of internal and external experts working hard to investigate these apps as quickly as possible. As of early June 2018, thousands of apps have been investigated and around 200 apps have been suspended—pending a thorough investigation into whether they did in fact misuse any data. Where we find evidence that these or other apps did misuse data, we will ban them and let people know.

Facebook is generally not opposed to regulation but wants to ensure it is the right regulation. The issues facing the industry are complex, multi-faceted, and affect an important part of peoples' lives. As such, Facebook is absolutely committed to working with regulators, like Congress, to craft the right regulations. Facebook would be happy to review any proposed legislation and provide comments.

54. Given your business model, how can you guarantee that this will not happen again?

To build a secure product with extensive infrastructure that connects people wherever they live or whatever their income level, we need to make sure everyone can afford it. Advertising lets us keep Facebook free, which ensures it remains affordable for everyone. We also believe the ads you see across the Facebook family of apps and services should be useful and relevant to you. Users can't opt out of seeing ads altogether because selling ads is what keeps Facebook free, but they do have different options to control how their data can and can't be used to show them ads. They're all found in ad preferences, which allows users to turn off the use of all data collected from partners off Facebook to target ads. Users can also decide which of their profile fields they want used for ad targeting in the Information section under "About you." Users can remove themselves from interests under "Your interests" and categories under "Your categories." And, we do not sell people's information to anyone, and we never will.

Facebook is committed to transparency for all ads, including ads with political content. Facebook believes that people should be able to easily understand why they are seeing ads, who paid for them, and what other ads those advertisers are running. As such, Facebook only allows authorized advertisers to run ads about elections or issues that are being debated across the country. In order to be authorized by Facebook, advertisers will need to confirm their identity and location. Furthermore, all political and issue ads will include a disclosure which reads: "Paid for by," and when users click on this disclosure they will be able to see details about the

advertiser. Users will also be able to see an explanation of why they saw the particular ad. This is similar to the disclosure included on political TV advertisements. We just launched globally View Active Ads, a feature that will enable anyone to see all of the ads an advertiser is currently running by visiting the advertiser's Facebook Page.

55. Why did you not foresee this and prevent it?

Facebook's policies regarding third-party usage of its platform technologies have prohibited—and continue to prohibit—third-party app developers from selling or licensing user data accessed from Facebook and from sharing any user data accessed from Facebook with any ad network, data broker or other advertising or monetization-related service. We take action on potential violations of our Platform Policies based on proactive review, external reports, and other signals. Kogan was not permitted to sell or transfer data to third-parties for the purposes he did. In doing so, Kogan and his company violated Facebook's Platform Policies.

On December 11, 2015, *The Guardian* published an article reporting that Kogan and his company, GSR, may have passed information the app had obtained from Facebook users to SCL Elections Ltd. (SCL)/Cambridge Analytica. Facebook immediately banned Kogan's app from our platform and investigated what happened and what further action Facebook should take to enforce our Platform Policies. Facebook considered the matter closed after obtaining written certifications and confirmations from Kogan, GSR, Cambridge Analytica, and SCL declaring that all such data they had obtained was accounted for and destroyed. We did not have any reason to affirmatively question the veracity of any of these certifications until March 2018, when we learned from media reporting that questions had been raised concerning the accuracy of the certifications. Facebook immediately banned Cambridge Analytica and SCL from purchasing advertisements on our services as well as removed the personal accounts of some of their officers. Moreover, while Facebook's policies in place at the time allowed us to audit apps to ensure that they were safe and did not violate its terms, we had already terminated Kogan's app's access to Facebook. Accordingly, there were no ongoing concerns about the level of data that app could access or might access in the future. With the benefit of hindsight, we wish we had notified people whose information may have been impacted. Facebook has since notified all people potentially impacted with a detailed notice at the top of their News Feed.

56. What is Facebook doing to make sure this doesn't happen again?

We believe everyone deserves good privacy controls. A user owns the information they share on Facebook. This means they decide what they share and who they share it with on Facebook, and they can change their mind. We require websites and apps who use our tools to tell users they're collecting and sharing their information with us, and to get users' permission to do so.

Everyone has the right to expect strong protections for their information. We also need to do our part to help keep our community safe, in a way that's consistent with people's privacy expectations. We've recently announced several steps to give people more control over their privacy, including a new Privacy Shortcuts tool that we're rolling out now to give people information about how to control their information, including choosing who can see what they post and adding protections like two-factor authentication to their account. People can learn more

about how to protect their privacy in our updated Data Policy and in our Privacy Basics feature (https://www.facebook.com/about/basics).

We are in the process of investigating every app that had access to a large amount of information before we changed our Platform in 2014. The investigation process is in full swing. We have large teams of internal and external experts working hard to investigate these apps as quickly as possible. As of early June 2018, thousands of apps have been investigated and around 200 apps have been suspended—pending a thorough investigation into whether they did in fact misuse any data. Where we find evidence that these or other apps did misuse data, we will ban them and let people know.

Facebook is generally not opposed to regulation but wants to ensure it is the right regulation. The issues facing the industry are complex, multi-faceted, and affect an important part of peoples' lives. As such, Facebook is absolutely committed to working with regulators, like Congress, to craft the right regulations. Facebook would be happy to review any proposed legislation and provide comments.

57. Walk us through concrete steps of how such abuse will be stopped in the future.

Facebook's policies regarding third-party usage of its platform technologies have prohibited—and continue to prohibit—third-party app developers from selling or licensing user data obtained from Facebook and from sharing any user data obtained from Facebook with any ad network, data broker or other advertising or monetization-related service.

We use a variety of tools to enforce Facebook policies against violating parties, including developers. We review tens of thousands of apps per year and regularly disapprove noncompliant apps as part of our proactive review process. We also use tools like cease and desist letters, account suspensions, letter agreements, and civil litigation. For example, since 2006, Facebook has sent over 1,150 cease-and-desist letters to over 1,600 targets. In 2017, we took action against about 370,000 apps, ranging from imposing certain restrictions to removal of the app from the platform. Moreover, we have required parties who have procured our data without authorization to delete that data. We have invested significant resources in these efforts.

Recently, we announced a number of additional steps we're taking to address concerns raised by Kogan's app.

- **Review our platform.** We will investigate all apps that had access to large amounts of data before the platform changes we announced in 2014, and we will audit any app where we identify suspicious activity. If we identify misuses of data, we'll take immediate action, including banning the app from our platform and pursuing legal action if appropriate.

- **Tell people about data misuse.** We will tell people about apps that have misused their data. This includes building a way for people to know if their data might have been accessed via the app. Moving forward, if we remove an app, we will tell people.

- **Turn off access for unused apps.** If someone has not used an app within the last three months, we will turn off the app's access to their data.

- **Restrict Facebook Login data.** We are changing Login, so that the only data that an app can request without app review will include name, profile photo, and email address. Requesting any other data will require approval from Facebook. We will also no longer allow apps to ask for access to information like religious or political views, relationship status and details, custom friends lists, education and work history, fitness activity, book reading and music listening activity, news reading, video watch activity, and games activity. We will encourage people to manage the apps they use. We already show people what apps their accounts are connected to and allow them to control what data they've permitted those apps to use. But we're making it easier for people to see what apps they use and the information they have shared with those apps.

- **Reward people who find vulnerabilities.** We launched the Data Abuse Bounty program so that people can report to us any misuses of data by app developers.

- **Update our policies.** We have updated our terms and Data Policy to explain how we use data and how data is shared with app developers.

58. Will the Facebook board of directors be holding any extra meetings over the next few months to deal with this new set of challenges?

We recognize that we have made mistakes, and we are committed to learning from this experience to secure our platform further and make our community safer for everyone going forward. As our CEO Mark Zuckerberg has said, when you are building something unprecedented like Facebook, there are going to be mistakes. What people should hold us accountable for is learning from the mistakes and continually doing better—and, at the end of the day, making sure that we're building things that people like and that make their lives better.

Particularly in the past few months, we've realized that we need to take a broader view of our responsibility to our community. Part of that effort is continuing our ongoing efforts to identify ways that we can improve our privacy practices. We've heard loud and clear that privacy settings and other important tools are too hard to find and that we must do more to keep people informed. So, we're taking additional steps to put people more in control of their privacy. For instance, we redesigned our entire settings menu on mobile devices from top to bottom to make things easier to find. We also created a new Privacy Shortcuts in a menu where users can control their data in just a few taps, with clearer explanations of how our controls work. The experience is now clearer, more visual, and easy-to-find. Furthermore, we also updated our terms of service that include our commitments to everyone using Facebook. We explain the services we offer in language that's easier to read. We've also updated our Data Policy to better spell out what data we collect and how we use it in Facebook, Instagram, Messenger, and other products.

59. After these issues are resolved would you take it upon yourself to ensure that companies advertising on Facebook are not predators exploiting the public for unnecessary monetary gain?

To build a secure product with extensive infrastructure that connects people wherever they live or whatever their income level, we need to make sure everyone can afford it. Advertising lets us keep Facebook free, which ensures it remains affordable for everyone. We also believe the ads you see across the Facebook family of apps and services should be useful and relevant to you. Users can't opt out of seeing ads altogether because selling ads is what keeps Facebook free, but they do have different options to control how their data can and can't be used to show them ads. They're all found in ad preferences, which allows users to turn off the use of all data collected from partners off Facebook to target ads. Users can also decide which of their profile fields they want used for ad targeting in the Information section under "About you." Users can remove themselves from interests under "Your interests" and categories under "Your categories." And, we do not sell people's information to anyone, and we never will.

Facebook is committed to transparency for all ads, including ads with political content. Facebook believes that people should be able to easily understand why they are seeing ads, who paid for them, and what other ads those advertisers are running. As such, Facebook only allows authorized advertisers to run ads about elections or issues that are being debated across the country. In order to be authorized by Facebook, advertisers will need to confirm their identity and location. Furthermore, all political and issue ads will include a disclosure which reads: "Paid for by," and when users click on this disclosure they will be able to see details about the advertiser. Users will also be able to see an explanation of why they saw the particular ad. This is similar to the disclosure included on political TV advertisements. We just launched globally View Active Ads, a feature that will enable anyone to see all of the ads an advertiser is currently running by visiting the advertiser's Facebook Page.

60. What security will be applied to your software to avoid a reoccurrence?

We believe everyone deserves good privacy controls. A user owns the information they share on Facebook. This means they decide what they share and who they share it with on Facebook, and they can change their mind. We require websites and apps who use our tools to tell users they're collecting and sharing their information with us, and to get users' permission to do so.

Everyone has the right to expect strong protections for their information. We also need to do our part to help keep our community safe, in a way that's consistent with people's privacy expectations. We've recently announced several steps to give people more control over their privacy, including a new Privacy Shortcuts tool that we're rolling out now to give people information about how to control their information, including choosing who can see what they post and adding protections like two-factor authentication to their account. People can learn more about how to protect their privacy in our updated Data Policy and in our Privacy Basics feature (https://www.facebook.com/about/basics).

We are in the process of investigating every app that had access to a large amount of information before we changed our Platform in 2014. The investigation process is in full swing. We have large teams of internal and external experts working hard to investigate these apps as quickly as possible. As of early June 2018, thousands of apps have been investigated and around 200 apps have been suspended—pending a thorough investigation into whether they did in fact

misuse any data. Where we find evidence that these or other apps did misuse data, we will ban them and let people know.

Facebook is generally not opposed to regulation but wants to ensure it is the right regulation. The issues facing the industry are complex, multi-faceted, and affect an important part of peoples' lives. As such, Facebook is absolutely committed to working with regulators, like Congress, to craft the right regulations. Facebook would be happy to review any proposed legislation and provide comments.

61. Precisely, what will Facebook do to allow users to control what companies/apps have access to data?

We believe everyone deserves good privacy controls. A user owns the information they share on Facebook. This means they decide what they share and who they share it with on Facebook, and they can change their mind. We require websites and apps who use our tools to tell users they're collecting and sharing their information with us, and to get users' permission to do so.

Everyone has the right to expect strong protections for their information. We also need to do our part to help keep our community safe, in a way that's consistent with people's privacy expectations. We've recently announced several steps to give people more control over their privacy, including a new Privacy Shortcuts tool that we're rolling out now to give people information about how to control their information, including choosing who can see what they post and adding protections like two-factor authentication to their account. People can learn more about how to protect their privacy in our updated Data Policy and in our Privacy Basics feature (https://www.facebook.com/about/basics).

We are in the process of investigating every app that had access to a large amount of information before we changed our Platform in 2014. The investigation process is in full swing. We have large teams of internal and external experts working hard to investigate these apps as quickly as possible. As of early June 2018, thousands of apps have been investigated and around 200 apps have been suspended—pending a thorough investigation into whether they did in fact misuse any data. Where we find evidence that these or other apps did misuse data, we will ban them and let people know.

Facebook is generally not opposed to regulation but wants to ensure it is the right regulation. The issues facing the industry are complex, multi-faceted, and affect an important part of peoples' lives. As such, Facebook is absolutely committed to working with regulators, like Congress, to craft the right regulations. Facebook would be happy to review any proposed legislation and provide comments.

62. How will you ensure that user's data is protected from now on so that this sort of egregious activity will not recur and have safeguards in place by (date to be set by your committee)?

We believe everyone deserves good privacy controls. A user owns the information they share on Facebook. This means they decide what they share and who they share it with on Facebook, and they can change their mind. We require websites and apps who use our tools to

tell users they're collecting and sharing their information with us, and to get users' permission to do so.

Everyone has the right to expect strong protections for their information. We also need to do our part to help keep our community safe, in a way that's consistent with people's privacy expectations. We've recently announced several steps to give people more control over their privacy, including a new Privacy Shortcuts tool that we're rolling out now to give people information about how to control their information, including choosing who can see what they post and adding protections like two-factor authentication to their account. People can learn more about how to protect their privacy in our updated Data Policy and in our Privacy Basics feature (https://www.facebook.com/about/basics).

We are in the process of investigating every app that had access to a large amount of information before we changed our Platform in 2014. The investigation process is in full swing. We have large teams of internal and external experts working hard to investigate these apps as quickly as possible. As of early June 2018, thousands of apps have been investigated and around 200 apps have been suspended—pending a thorough investigation into whether they did in fact misuse any data. Where we find evidence that these or other apps did misuse data, we will ban them and let people know.

Facebook is generally not opposed to regulation but wants to ensure it is the right regulation. The issues facing the industry are complex, multi-faceted, and affect an important part of peoples' lives. As such, Facebook is absolutely committed to working with regulators, like Congress, to craft the right regulations. Facebook would be happy to review any proposed legislation and provide comments.

63. What kind of policies will you put in place to protect the people using Facebook? How will you test?

We believe everyone deserves good privacy controls. A user owns the information they share on Facebook. This means they decide what they share and who they share it with on Facebook, and they can change their mind. We require websites and apps who use our tools to tell users they're collecting and sharing their information with us, and to get users' permission to do so.

Everyone has the right to expect strong protections for their information. We also need to do our part to help keep our community safe, in a way that's consistent with people's privacy expectations. We've recently announced several steps to give people more control over their privacy, including a new Privacy Shortcuts tool that we're rolling out now to give people information about how to control their information, including choosing who can see what they post and adding protections like two-factor authentication to their account. People can learn more about how to protect their privacy in our updated Data Policy and in our Privacy Basics feature (https://www.facebook.com/about/basics).

We are in the process of investigating every app that had access to a large amount of information before we changed our Platform in 2014. The investigation process is in full swing. We have large teams of internal and external experts working hard to investigate these apps as

quickly as possible. As of early June 2018, thousands of apps have been investigated and around 200 apps have been suspended—pending a thorough investigation into whether they did in fact misuse any data. Where we find evidence that these or other apps did misuse data, we will ban them and let people know.

Facebook is generally not opposed to regulation but wants to ensure it is the right regulation. The issues facing the industry are complex, multi-faceted, and affect an important part of peoples' lives. As such, Facebook is absolutely committed to working with regulators, like Congress, to craft the right regulations. Facebook would be happy to review any proposed legislation and provide comments.

64. How will you ensure users are aware, consenting, and involved in changes that impact their privacy?

We believe everyone deserves good privacy controls. A user owns the information they share on Facebook. This means they decide what they share and who they share it with on Facebook, and they can change their mind. We require websites and apps who use our tools to tell users they're collecting and sharing their information with us, and to get users' permission to do so.

Everyone has the right to expect strong protections for their information. We also need to do our part to help keep our community safe, in a way that's consistent with people's privacy expectations. We've recently announced several steps to give people more control over their privacy, including a new Privacy Shortcuts tool that we're rolling out now to give people information about how to control their information, including choosing who can see what they post and adding protections like two-factor authentication to their account. People can learn more about how to protect their privacy in our updated Data Policy and in our Privacy Basics feature (https://www.facebook.com/about/basics).

We are in the process of investigating every app that had access to a large amount of information before we changed our Platform in 2014. The investigation process is in full swing. We have large teams of internal and external experts working hard to investigate these apps as quickly as possible. As of early June 2018, thousands of apps have been investigated and around 200 apps have been suspended—pending a thorough investigation into whether they did in fact misuse any data. Where we find evidence that these or other apps did misuse data, we will ban them and let people know.

Facebook is generally not opposed to regulation but wants to ensure it is the right regulation. The issues facing the industry are complex, multi-faceted, and affect an important part of peoples' lives. As such, Facebook is absolutely committed to working with regulators, like Congress, to craft the right regulations. Facebook would be happy to review any proposed legislation and provide comments.

65. What steps is Facebook taking to make sure our data is not shared without our permission? Why should we believe you?

We believe everyone deserves good privacy controls. A user owns the information they share on Facebook. This means they decide what they share and who they share it with on

Facebook, and they can change their mind. We require websites and apps who use our tools to tell users they're collecting and sharing their information with us, and to get users' permission to do so.

Everyone has the right to expect strong protections for their information. We also need to do our part to help keep our community safe, in a way that's consistent with people's privacy expectations. We've recently announced several steps to give people more control over their privacy, including a new Privacy Shortcuts tool that we're rolling out now to give people information about how to control their information, including choosing who can see what they post and adding protections like two-factor authentication to their account. People can learn more about how to protect their privacy in our updated Data Policy and in our Privacy Basics feature (https://www.facebook.com/about/basics).

We are in the process of investigating every app that had access to a large amount of information before we changed our Platform in 2014. The investigation process is in full swing. We have large teams of internal and external experts working hard to investigate these apps as quickly as possible. As of early June 2018, thousands of apps have been investigated and around 200 apps have been suspended—pending a thorough investigation into whether they did in fact misuse any data. Where we find evidence that these or other apps did misuse data, we will ban them and let people know.

Facebook is generally not opposed to regulation but wants to ensure it is the right regulation. The issues facing the industry are complex, multi-faceted, and affect an important part of peoples' lives. As such, Facebook is absolutely committed to working with regulators, like Congress, to craft the right regulations. Facebook would be happy to review any proposed legislation and provide comments.

66. What will he do to make sure this doesn't happen again?

Facebook's policies regarding third-party usage of its platform technologies have prohibited—and continue to prohibit—third-party app developers from selling or licensing user data obtained from Facebook and from sharing any user data obtained from Facebook with any ad network, data broker or other advertising or monetization-related service.

We use a variety of tools to enforce Facebook policies against violating parties, including developers. We review tens of thousands of apps per year and regularly disapprove noncompliant apps as part of our proactive review process. We also use tools like cease and desist letters, account suspensions, letter agreements, and civil litigation. For example, since 2006, Facebook has sent over 1,150 cease-and-desist letters to over 1,600 targets. In 2017, we took action against about 370,000 apps, ranging from imposing certain restrictions to removal of the app from the platform. Moreover, we have required parties who have procured our data without authorization to delete that data. We have invested significant resources in these efforts.

Recently, we announced a number of additional steps we're taking to address concerns raised by Kogan's app.

- **Review our platform.** We will investigate all apps that had access to large amounts of data before the platform changes we announced in 2014, and we will audit any app where we identify suspicious activity. If we identify misuses of data, we'll take immediate action, including banning the app from our platform and pursuing legal action if appropriate.

- **Tell people about data misuse.** We will tell people about apps that have misused their data. This includes building a way for people to know if their data might have been accessed via the app. Moving forward, if we remove an app, we will tell people.

- **Turn off access for unused apps.** If someone has not used an app within the last three months, we will turn off the app's access to their data.

- **Restrict Facebook Login data.** We are changing Login, so that the only data that an app can request without app review will include name, profile photo, and email address. Requesting any other data will require approval from Facebook. We will also no longer allow apps to ask for access to information like religious or political views, relationship status and details, custom friends lists, education and work history, fitness activity, book reading and music listening activity, news reading, video watch activity, and games activity. We will encourage people to manage the apps they use. We already show people what apps their accounts are connected to and allow them to control what data they've permitted those apps to use. But we're making it easier for people to see what apps they use and the information they have shared with those apps.

- **Reward people who find vulnerabilities.** We launched the Data Abuse Bounty program so that people can report to us any misuses of data by app developers.

- **Update our policies.** We have updated our terms and Data Policy to explain how we use data and how data is shared with app developers.

67. Will you be reporting your progress to the public on a regular basis?

We believe everyone deserves good privacy controls. A user owns the information they share on Facebook. This means they decide what they share and who they share it with on Facebook, and they can change their mind. We require websites and apps who use our tools to tell users they're collecting and sharing their information with us, and to get users' permission to do so.

Everyone has the right to expect strong protections for their information. We also need to do our part to help keep our community safe, in a way that's consistent with people's privacy expectations. We've recently announced several steps to give people more control over their privacy, including a new Privacy Shortcuts tool that we're rolling out now to give people information about how to control their information, including choosing who can see what they post and adding protections like two-factor authentication to their account. People can learn more about how to protect their privacy in our updated Data Policy and in our Privacy Basics feature (https://www.facebook.com/about/basics).

We are in the process of investigating every app that had access to a large amount of information before we changed our Platform in 2014. The investigation process is in full swing. We have large teams of internal and external experts working hard to investigate these apps as quickly as possible. As of early June 2018, thousands of apps have been investigated and around 200 apps have been suspended—pending a thorough investigation into whether they did in fact misuse any data. Where we find evidence that these or other apps did misuse data, we will ban them and let people know.

Facebook is generally not opposed to regulation but wants to ensure it is the right regulation. The issues facing the industry are complex, multi-faceted, and affect an important part of peoples' lives. As such, Facebook is absolutely committed to working with regulators, like Congress, to craft the right regulations. Facebook would be happy to review any proposed legislation and provide comments.

68. How are you going to change your business model to protect customer data, give customers control over it, not give third parties access to it without explicit permission, and remove the incentive to seek maximum monetization of customer data.

We believe that it's important to communicate with people about the information that we collect and how people can control it. As explained in our Data Policy, we collect three basic categories of data about people:

(1) data about things people do and share (and who they connect with) on our services;

(2) data about the devices people use to access our services; and

(3) data we receive from partners, including the websites and apps that use our business tools.

We collect information about the people, Pages, accounts, hashtags, and groups users are connected to and how they interact with them across our Products, such as people a user communicates with the most or groups users are part of. We also collect contact information if they choose to upload, sync, or import it from a device (such as an address book or call log or SMS log history), which we use for things like helping them and others find people they may know.

The data we use to show ads to people depends on the data we have received from people. For people who are new to Facebook, we may have minimal data that we can use. For people who have used our services for longer, we likely have more data, but the amount of data will depend on the nature of that use and how they have used our controls. Any person can see each of the specific interests we maintain about them for advertising by visiting Ads Preferences, which lets people see what interests we use to choose ads for them—and to edit or delete these interests. We also provide more detailed information about how we use data to decide what ads to show to people in our "About Facebook Ads" page, at https://www.facebook.com/ads/about. And, we do not sell people's information to anyone, and we never will.

All users must expressly consent to Facebook's Terms and Data Policy when registering for Facebook. The Data Policy explains the kinds of information we collect, how we use this information, how we share this information, and how users can manage and delete information.

Facebook does not create profiles for people without a Facebook account, but we do receive some information from devices and browsers that may be used by non-users. For example:

- When people visit apps or websites that feature our technologies—like the Facebook Like or Comment button—our servers automatically log (i) standard browser or app records of the fact that a particular device or user visited the website or app (this connection to Facebook's servers occurs automatically when a person visits a website or app that contains our technologies, such as a Like button, and is an inherent function of Internet design); and (ii) any additional information the publisher of the app or website chooses to share with Facebook about the person's activities on that site (such as the fact that a purchase was made on the site). This is a standard feature of the Internet, and most websites and apps share this same information with multiple different third-parties whenever people visit their website or app. When the person visiting a website featuring Facebook's tools is not a registered Facebook user, Facebook does not have information identifying that individual, and it does not create profiles for this individual.

- We also may receive information about the device of a non-registered user if that user visits a part of Facebook that does not require people to log in—such as a public Facebook Page. The information we log when people visit our websites or apps is the same as described above and is the same information that any provider of an online service would receive.

- In addition, Facebook may receive some basic information about devices where Facebook apps are installed, including before people using those devices have registered for Facebook (such as when a user downloads a Facebook app, but has not yet created an account, or if the app is preloaded on a given device). This device data includes things like device model, operating system, IP address, app version and device identifiers. We use this information to provide the right version of the app, help people who want to create accounts (for example, optimizing the registration flow for the specific device), retrieving bug fixes and measuring and improving app performance. We do not use this information to build profiles about non-registered users.

69. Are you solving this privacy issue at the ethical level or just the one technical level that caused the current problem?

We believe everyone deserves good privacy controls. A user owns the information they share on Facebook. This means they decide what they share and who they share it with on Facebook, and they can change their mind. We require websites and apps who use our tools to tell users they're collecting and sharing their information with us, and to get users' permission to do so.

Everyone has the right to expect strong protections for their information. We also need to do our part to help keep our community safe, in a way that's consistent with people's privacy expectations. We've recently announced several steps to give people more control over their privacy, including a new Privacy Shortcuts tool that we're rolling out now to give people information about how to control their information, including choosing who can see what they post and adding protections like two-factor authentication to their account. People can learn more about how to protect their privacy in our updated Data Policy and in our Privacy Basics feature (https://www.facebook.com/about/basics).

We are in the process of investigating every app that had access to a large amount of information before we changed our Platform in 2014. The investigation process is in full swing. We have large teams of internal and external experts working hard to investigate these apps as quickly as possible. As of early June 2018, thousands of apps have been investigated and around 200 apps have been suspended—pending a thorough investigation into whether they did in fact misuse any data. Where we find evidence that these or other apps did misuse data, we will ban them and let people know.

Facebook is generally not opposed to regulation but wants to ensure it is the right regulation. The issues facing the industry are complex, multi-faceted, and affect an important part of peoples' lives. As such, Facebook is absolutely committed to working with regulators, like Congress, to craft the right regulations. Facebook would be happy to review any proposed legislation and provide comments.

70. What safeguards is he putting in place so this doesn't happen again?

Facebook's policies regarding third-party usage of its platform technologies have prohibited—and continue to prohibit—third-party app developers from selling or licensing user data obtained from Facebook and from sharing any user data obtained from Facebook with any ad network, data broker or other advertising or monetization-related service.

We use a variety of tools to enforce Facebook policies against violating parties, including developers. We review tens of thousands of apps per year and regularly disapprove noncompliant apps as part of our proactive review process. We also use tools like cease and desist letters, account suspensions, letter agreements, and civil litigation. For example, since 2006, Facebook has sent over 1,150 cease-and-desist letters to over 1,600 targets. In 2017, we took action against about 370,000 apps, ranging from imposing certain restrictions to removal of the app from the platform. Moreover, we have required parties who have procured our data without authorization to delete that data. We have invested significant resources in these efforts.

Recently, we announced a number of additional steps we're taking to address concerns raised by Kogan's app.

- **Review our platform.** We will investigate all apps that had access to large amounts of data before the platform changes we announced in 2014, and we will audit any app where we identify suspicious activity. If we identify misuses of data, we'll take immediate action, including banning the app from our platform and pursuing legal action if appropriate.

- **Tell people about data misuse.** We will tell people about apps that have misused their data. This includes building a way for people to know if their data might have been accessed via the app. Moving forward, if we remove an app, we will tell people.

- **Turn off access for unused apps.** If someone has not used an app within the last three months, we will turn off the app's access to their data.

- **Restrict Facebook Login data.** We are changing Login, so that the only data that an app can request without app review will include name, profile photo, and email address. Requesting any other data will require approval from Facebook. We will also no longer allow apps to ask for access to information like religious or political views, relationship status and details, custom friends lists, education and work history, fitness activity, book reading and music listening activity, news reading, video watch activity, and games activity. We will encourage people to manage the apps they use. We already show people what apps their accounts are connected to and allow them to control what data they've permitted those apps to use. But we're making it easier for people to see what apps they use and the information they have shared with those apps.

- **Reward people who find vulnerabilities.** We launched the Data Abuse Bounty program so that people can report to us any misuses of data by app developers.

- **Update our policies.** We have updated our terms and Data Policy to explain how we use data and how data is shared with app developers.

71. Will you, Mr. FB CEO, provide a published Telephone # & Account Assistance Resource for All Users?

We believe that it's important to communicate with people about the information that we collect and how people can control it. As explained in our Data Policy, we collect three basic categories of data about people:

(1) data about things people do and share (and who they connect with) on our services;

(2) data about the devices people use to access our services; and

(3) data we receive from partners, including the websites and apps that use our business tools.

We collect information about the people, Pages, accounts, hashtags, and groups users are connected to and how they interact with them across our Products, such as people a user communicates with the most or groups users are part of. We also collect contact information if they choose to upload, sync, or import it from a device (such as an address book or call log or SMS log history), which we use for things like helping them and others find people they may know.

The data we use to show ads to people depends on the data we have received from people. For people who are new to Facebook, we may have minimal data that we can use. For people who have used our services for longer, we likely have more data, but the amount of data will depend on the nature of that use and how they have used our controls. Any person can see each of the specific interests we maintain about them for advertising by visiting Ads Preferences, which lets people see what interests we use to choose ads for them—and to edit or delete these interests. We also provide more detailed information about how we use data to decide what ads to show to people in our "About Facebook Ads" page, at https://www.facebook.com/ads/about. And, we do not sell people's information to anyone, and we never will.

All users must expressly consent to Facebook's Terms and Data Policy when registering for Facebook. The Data Policy explains the kinds of information we collect, how we use this information, how we share this information, and how users can manage and delete information.

Facebook does not create profiles for people without a Facebook account, but we do receive some information from devices and browsers that may be used by non-users. For example:

- When people visit apps or websites that feature our technologies—like the Facebook Like or Comment button—our servers automatically log (i) standard browser or app records of the fact that a particular device or user visited the website or app (this connection to Facebook's servers occurs automatically when a person visits a website or app that contains our technologies, such as a Like button, and is an inherent function of Internet design); and (ii) any additional information the publisher of the app or website chooses to share with Facebook about the person's activities on that site (such as the fact that a purchase was made on the site). This is a standard feature of the Internet, and most websites and apps share this same information with multiple different third-parties whenever people visit their website or app. When the person visiting a website featuring Facebook's tools is not a registered Facebook user, Facebook does not have information identifying that individual, and it does not create profiles for this individual.

- We also may receive information about the device of a non-registered user if that user visits a part of Facebook that does not require people to log in—such as a public Facebook Page. The information we log when people visit our websites or apps is the same as described above and is the same information that any provider of an online service would receive.

- In addition, Facebook may receive some basic information about devices where Facebook apps are installed, including before people using those devices have registered for Facebook (such as when a user downloads a Facebook app, but has not yet created an account, or if the app is preloaded on a given device). This device data includes things like device model, operating system, IP address, app version and device identifiers. We use this information to provide the right version of the app, help people who want to create accounts (for example, optimizing the registration flow for the specific device), retrieving bug fixes and measuring and improving app performance. We do not use this information to build profiles about non-registered users.

72. When did he go back on his promise to keep Facebook users' data private?

We believe that it's important to communicate with people about the information that we collect and how people can control it. As explained in our Data Policy, we collect three basic categories of data about people:

(1) data about things people do and share (and who they connect with) on our services;

(2) data about the devices people use to access our services; and

(3) data we receive from partners, including the websites and apps that use our business tools.

We collect information about the people, Pages, accounts, hashtags, and groups users are connected to and how they interact with them across our Products, such as people a user communicates with the most or groups users are part of. We also collect contact information if they choose to upload, sync, or import it from a device (such as an address book or call log or SMS log history), which we use for things like helping them and others find people they may know.

The data we use to show ads to people depends on the data we have received from people. For people who are new to Facebook, we may have minimal data that we can use. For people who have used our services for longer, we likely have more data, but the amount of data will depend on the nature of that use and how they have used our controls. Any person can see each of the specific interests we maintain about them for advertising by visiting Ads Preferences, which lets people see what interests we use to choose ads for them—and to edit or delete these interests. We also provide more detailed information about how we use data to decide what ads to show to people in our "About Facebook Ads" page, at https://www.facebook.com/ads/about. And, we do not sell people's information to anyone, and we never will.

All users must expressly consent to Facebook's Terms and Data Policy when registering for Facebook. The Data Policy explains the kinds of information we collect, how we use this information, how we share this information, and how users can manage and delete information.

Facebook does not create profiles for people without a Facebook account, but we do receive some information from devices and browsers that may be used by non-users. For example:

- When people visit apps or websites that feature our technologies—like the Facebook Like or Comment button—our servers automatically log (i) standard browser or app records of the fact that a particular device or user visited the website or app (this connection to Facebook's servers occurs automatically when a person visits a website or app that contains our technologies, such as a Like button, and is an inherent function of Internet design); and (ii) any additional information the publisher of the app or website chooses to share with Facebook about the person's activities on that site (such as the fact that a purchase was made on the site). This is a standard feature of the Internet, and most websites and apps share this same information with multiple different third-parties

whenever people visit their website or app. When the person visiting a website featuring Facebook's tools is not a registered Facebook user, Facebook does not have information identifying that individual, and it does not create profiles for this individual.

- We also may receive information about the device of a non-registered user if that user visits a part of Facebook that does not require people to log in—such as a public Facebook Page. The information we log when people visit our websites or apps is the same as described above and is the same information that any provider of an online service would receive.

- In addition, Facebook may receive some basic information about devices where Facebook apps are installed, including before people using those devices have registered for Facebook (such as when a user downloads a Facebook app, but has not yet created an account, or if the app is preloaded on a given device). This device data includes things like device model, operating system, IP address, app version and device identifiers. We use this information to provide the right version of the app, help people who want to create accounts (for example, optimizing the registration flow for the specific device), retrieving bug fixes and measuring and improving app performance. We do not use this information to build profiles about non-registered users.

73. Does Facebook have adequate policies in place to ensure both privacy and security?

We believe everyone deserves good privacy controls. A user owns the information they share on Facebook. This means they decide what they share and who they share it with on Facebook, and they can change their mind. We require websites and apps who use our tools to tell users they're collecting and sharing their information with us, and to get users' permission to do so.

Everyone has the right to expect strong protections for their information. We also need to do our part to help keep our community safe, in a way that's consistent with people's privacy expectations. We've recently announced several steps to give people more control over their privacy, including a new Privacy Shortcuts tool that we're rolling out now to give people information about how to control their information, including choosing who can see what they post and adding protections like two-factor authentication to their account. People can learn more about how to protect their privacy in our updated Data Policy and in our Privacy Basics feature (https://www.facebook.com/about/basics).

We are in the process of investigating every app that had access to a large amount of information before we changed our Platform in 2014. The investigation process is in full swing. We have large teams of internal and external experts working hard to investigate these apps as quickly as possible. As of early June 2018, thousands of apps have been investigated and around 200 apps have been suspended—pending a thorough investigation into whether they did in fact misuse any data. Where we find evidence that these or other apps did misuse data, we will ban them and let people know.

Facebook is generally not opposed to regulation but wants to ensure it is the right regulation. The issues facing the industry are complex, multi-faceted, and affect an important

part of peoples' lives. As such, Facebook is absolutely committed to working with regulators, like Congress, to craft the right regulations. Facebook would be happy to review any proposed legislation and provide comments.

74. What steps has Facebook taken to correct the mistakes that have compromised the personal information of millions of Americans & other?

Facebook's policies regarding third-party usage of its platform technologies have prohibited—and continue to prohibit—third-party app developers from selling or licensing user data obtained from Facebook and from sharing any user data obtained from Facebook with any ad network, data broker or other advertising or monetization-related service.

We use a variety of tools to enforce Facebook policies against violating parties, including developers. We review tens of thousands of apps per year and regularly disapprove noncompliant apps as part of our proactive review process. We also use tools like cease and desist letters, account suspensions, letter agreements, and civil litigation. For example, since 2006, Facebook has sent over 1,150 cease-and-desist letters to over 1,600 targets. In 2017, we took action against about 370,000 apps, ranging from imposing certain restrictions to removal of the app from the platform. Moreover, we have required parties who have procured our data without authorization to delete that data. We have invested significant resources in these efforts.

Recently, we announced a number of additional steps we're taking to address concerns raised by Kogan's app.

- **Review our platform.** We will investigate all apps that had access to large amounts of data before the platform changes we announced in 2014, and we will audit any app where we identify suspicious activity. If we identify misuses of data, we'll take immediate action, including banning the app from our platform and pursuing legal action if appropriate.

- **Tell people about data misuse.** We will tell people about apps that have misused their data. This includes building a way for people to know if their data might have been accessed via the app. Moving forward, if we remove an app, we will tell people.

- **Turn off access for unused apps.** If someone has not used an app within the last three months, we will turn off the app's access to their data.

- **Restrict Facebook Login data.** We are changing Login, so that the only data that an app can request without app review will include name, profile photo, and email address. Requesting any other data will require approval from Facebook. We will also no longer allow apps to ask for access to information like religious or political views, relationship status and details, custom friends lists, education and work history, fitness activity, book reading and music listening activity, news reading, video watch activity, and games activity. We will encourage people to manage the apps they use. We already show people what apps their accounts are connected to and allow them to control what data they've permitted those apps to use. But we're making it easier for

people to see what apps they use and the information they have shared with those apps.

- **Reward people who find vulnerabilities.** We launched the Data Abuse Bounty program so that people can report to us any misuses of data by app developers.

- **Update our policies.** We have updated our terms and Data Policy to explain how we use data and how data is shared with app developers.

75. What steps are you taking to ensure the privacy of our data?

We believe everyone deserves good privacy controls. A user owns the information they share on Facebook. This means they decide what they share and who they share it with on Facebook, and they can change their mind. We require websites and apps who use our tools to tell users they're collecting and sharing their information with us, and to get users' permission to do so.

Everyone has the right to expect strong protections for their information. We also need to do our part to help keep our community safe, in a way that's consistent with people's privacy expectations. We've recently announced several steps to give people more control over their privacy, including a new Privacy Shortcuts tool that we're rolling out now to give people information about how to control their information, including choosing who can see what they post and adding protections like two-factor authentication to their account. People can learn more about how to protect their privacy in our updated Data Policy and in our Privacy Basics feature (https://www.facebook.com/about/basics).

We are in the process of investigating every app that had access to a large amount of information before we changed our Platform in 2014. The investigation process is in full swing. We have large teams of internal and external experts working hard to investigate these apps as quickly as possible. As of early June 2018, thousands of apps have been investigated and around 200 apps have been suspended—pending a thorough investigation into whether they did in fact misuse any data. Where we find evidence that these or other apps did misuse data, we will ban them and let people know.

Facebook is generally not opposed to regulation but wants to ensure it is the right regulation. The issues facing the industry are complex, multi-faceted, and affect an important part of peoples' lives. As such, Facebook is absolutely committed to working with regulators, like Congress, to craft the right regulations. Facebook would be happy to review any proposed legislation and provide comments.

76. What changes will be put in place to insure this does not happen again?

Facebook's policies regarding third-party usage of its platform technologies have prohibited—and continue to prohibit—third-party app developers from selling or licensing user data obtained from Facebook and from sharing any user data obtained from Facebook with any ad network, data broker or other advertising or monetization-related service.

We use a variety of tools to enforce Facebook policies against violating parties, including developers. We review tens of thousands of apps per year and regularly disapprove noncompliant apps as part of our proactive review process. We also use tools like cease and desist letters, account suspensions, letter agreements, and civil litigation. For example, since 2006, Facebook has sent over 1,150 cease-and-desist letters to over 1,600 targets. In 2017, we took action against about 370,000 apps, ranging from imposing certain restrictions to removal of the app from the platform. Moreover, we have required parties who have procured our data without authorization to delete that data. We have invested significant resources in these efforts.

Recently, we announced a number of additional steps we're taking to address concerns raised by Kogan's app.

- **Review our platform.** We will investigate all apps that had access to large amounts of data before the platform changes we announced in 2014, and we will audit any app where we identify suspicious activity. If we identify misuses of data, we'll take immediate action, including banning the app from our platform and pursuing legal action if appropriate.

- **Tell people about data misuse.** We will tell people about apps that have misused their data. This includes building a way for people to know if their data might have been accessed via the app. Moving forward, if we remove an app, we will tell people.

- **Turn off access for unused apps.** If someone has not used an app within the last three months, we will turn off the app's access to their data.

- **Restrict Facebook Login data.** We are changing Login, so that the only data that an app can request without app review will include name, profile photo, and email address. Requesting any other data will require approval from Facebook. We will also no longer allow apps to ask for access to information like religious or political views, relationship status and details, custom friends lists, education and work history, fitness activity, book reading and music listening activity, news reading, video watch activity, and games activity. We will encourage people to manage the apps they use. We already show people what apps their accounts are connected to and allow them to control what data they've permitted those apps to use. But we're making it easier for people to see what apps they use and the information they have shared with those apps.

- **Reward people who find vulnerabilities.** We launched the Data Abuse Bounty program so that people can report to us any misuses of data by app developers.

- **Update our policies.** We have updated our terms and Data Policy to explain how we use data and how data is shared with app developers.

77. Is Facebook going to fix this access problem immediately and completely and ensure that it never happens again?

Facebook's policies regarding third-party usage of its platform technologies have prohibited—and continue to prohibit—third-party app developers from selling or licensing user data obtained from Facebook and from sharing any user data obtained from Facebook with any ad network, data broker or other advertising or monetization-related service.

We use a variety of tools to enforce Facebook policies against violating parties, including developers. We review tens of thousands of apps per year and regularly disapprove noncompliant apps as part of our proactive review process. We also use tools like cease and desist letters, account suspensions, letter agreements, and civil litigation. For example, since 2006, Facebook has sent over 1,150 cease-and-desist letters to over 1,600 targets. In 2017, we took action against about 370,000 apps, ranging from imposing certain restrictions to removal of the app from the platform. Moreover, we have required parties who have procured our data without authorization to delete that data. We have invested significant resources in these efforts.

Recently, we announced a number of additional steps we're taking to address concerns raised by Kogan's app.

- **Review our platform.** We will investigate all apps that had access to large amounts of data before the platform changes we announced in 2014, and we will audit any app where we identify suspicious activity. If we identify misuses of data, we'll take immediate action, including banning the app from our platform and pursuing legal action if appropriate.

- **Tell people about data misuse.** We will tell people about apps that have misused their data. This includes building a way for people to know if their data might have been accessed via the app. Moving forward, if we remove an app, we will tell people.

- **Turn off access for unused apps.** If someone has not used an app within the last three months, we will turn off the app's access to their data.

- **Restrict Facebook Login data.** We are changing Login, so that the only data that an app can request without app review will include name, profile photo, and email address. Requesting any other data will require approval from Facebook. We will also no longer allow apps to ask for access to information like religious or political views, relationship status and details, custom friends lists, education and work history, fitness activity, book reading and music listening activity, news reading, video watch activity, and games activity. We will encourage people to manage the apps they use. We already show people what apps their accounts are connected to and allow them to control what data they've permitted those apps to use. But we're making it easier for people to see what apps they use and the information they have shared with those apps.

- **Reward people who find vulnerabilities.** We launched the Data Abuse Bounty program so that people can report to us any misuses of data by app developers.

- **Update our policies.** We have updated our terms and Data Policy to explain how we use data and how data is shared with app developers.

78. Will you fund fact checking on Facebook, and actively counter lies published as news?

We want Facebook to be a place where people can discover more news, information, and perspectives, and we are working to build products that help to that. Through our News Feed algorithm, we also work hard to actively reduce the distribution of clickbait, sensationalism, and misinformation, on the one hand, and to boost news and information from sources that are trusted, informative, and local, on the other hand.

We are focusing on four different strategies to address misinformation:

- **Strengthening enforcement of our authenticity policies.** We are investing heavily in new technology and hiring thousands more people to tackle the problem of inauthenticity on the platform. Fake accounts are often associated with false news, so this is an area that will have a huge impact on curbing the spread of inaccurate information.

- **Finding industry solutions.** All of us—from tech companies and media companies to newsrooms and classrooms—must work together to find industry solutions to strengthen the online news ecosystem and our own digital literacy. That's why we're collaborating with others who operate in this space. Last January, we announced The Facebook Journalism Project, an initiative that seeks to establish stronger ties between Facebook and the news industry. The project is focused on developing news products, providing training and tools for journalists, and working with publishers and educators on how we can equip people with the knowledge they need to be informed readers in the digital age. Since launching the Journalism Project, we've met with more than 2,600 publishers around the world to understand how they use our products and how we can make improvements to better support their needs.

- **Disrupting economic incentives.** When it comes to fighting false news, we've found that a lot of it is financially motivated. So, one of the most effective approaches is removing the economic incentives for those who traffic in inaccurate information. We've done things like block ads from pages that repeatedly share false news and significantly limit the distribution of web pages that deliver low quality web experiences.

- **Building new products.** We believe it's important to amplify the good effects of social media and mitigate the bad—to contribute to the diversity of ideas, information, and view points, while strengthening our common understanding.

    - We believe giving people more context can help them decide what to trust and what to share. The third-party fact-checking program we have developed uses reports from our community, along with other signals, to send stories to accredited third-party fact checking organizations. If the fact checking organizations identify a story as fake, we will suggest related articles in News Feed to show people different points of view, including information from fact checkers. Stories that have been disputed may also appear lower in News

Feed. Our own data analytics show that a false rating from one of our fact checking partners reduces future impressions on Facebook by 80 percent.

- We're also testing Article Context as a way of giving people more information about the material they're reading on Facebook. Since we launched this test, some of the articles people see in News Feed will feature an "i" icon that allows them to access more information at the tap of a button. The information we surface is pulled from across the internet, and includes things like the publisher's Wikipedia entry, trending articles or related articles about the topic, and information about how the article is being shared on Facebook. In some cases, if that information is unavailable, we will let people know since that can also be helpful context.

79. Is it possible as a fan of Facebook to have a location directly on our news feed fact checker on items posted to our page? This would help Facebook and users. What do you think should be done to Cambridge Analytica for causing this problem?

We want Facebook to be a place where people can discover more news, information, and perspectives, and we are working to build products that help to that. Through our News Feed algorithm, we also work hard to actively reduce the distribution of clickbait, sensationalism, and misinformation, on the one hand, and to boost news and information from sources that are trusted, informative, and local, on the other hand.

We are focusing on four different strategies to address misinformation:

- **Strengthening enforcement of our authenticity policies.** We are investing heavily in new technology and hiring thousands more people to tackle the problem of inauthenticity on the platform. Fake accounts are often associated with false news, so this is an area that will have a huge impact on curbing the spread of inaccurate information.

- **Finding industry solutions.** All of us—from tech companies and media companies to newsrooms and classrooms—must work together to find industry solutions to strengthen the online news ecosystem and our own digital literacy. That's why we're collaborating with others who operate in this space. Last January, we announced The Facebook Journalism Project, an initiative that seeks to establish stronger ties between Facebook and the news industry. The project is focused on developing news products, providing training and tools for journalists, and working with publishers and educators on how we can equip people with the knowledge they need to be informed readers in the digital age. Since launching the Journalism Project, we've met with more than 2,600 publishers around the world to understand how they use our products and how we can make improvements to better support their needs.

- **Disrupting economic incentives.** When it comes to fighting false news, we've found that a lot of it is financially motivated. So, one of the most effective approaches is removing the economic incentives for those who traffic in inaccurate information. We've done things like block ads from pages that repeatedly share false news and

significantly limit the distribution of web pages that deliver low quality web experiences.

- **Building new products.** We believe it's important to amplify the good effects of social media and mitigate the bad—to contribute to the diversity of ideas, information, and view points, while strengthening our common understanding.

    - We believe giving people more context can help them decide what to trust and what to share. The third-party fact-checking program we have developed uses reports from our community, along with other signals, to send stories to accredited third-party fact checking organizations. If the fact checking organizations identify a story as fake, we will suggest related articles in News Feed to show people different points of view, including information from fact checkers. Stories that have been disputed may also appear lower in News Feed. Our own data analytics show that a false rating from one of our fact checking partners reduces future impressions on Facebook by 80 percent.

    - We're also testing Article Context as a way of giving people more information about the material they're reading on Facebook. Since we launched this test, some of the articles people see in News Feed will feature an "i" icon that allows them to access more information at the tap of a button. The information we surface is pulled from across the internet, and includes things like the publisher's Wikipedia entry, trending articles or related articles about the topic, and information about how the article is being shared on Facebook. In some cases, if that information is unavailable, we will let people know since that can also be helpful context.

80. Are you willing to commit, today, to educating your users so they are both aware of the data you and other companies harvest, and are better able to be critical consumers of information online?

We believe that it's important to communicate with people about the information that we collect and how people can control it. As explained in our Data Policy, we collect three basic categories of data about people:

(1) data about things people do and share (and who they connect with) on our services;

(2) data about the devices people use to access our services; and

(3) data we receive from partners, including the websites and apps that use our business tools.

We collect information about the people, Pages, accounts, hashtags, and groups users are connected to and how they interact with them across our Products, such as people a user communicates with the most or groups users are part of. We also collect contact information if they choose to upload, sync, or import it from a device (such as an address book or call log or

SMS log history), which we use for things like helping them and others find people they may know.

The data we use to show ads to people depends on the data we have received from people. For people who are new to Facebook, we may have minimal data that we can use. For people who have used our services for longer, we likely have more data, but the amount of data will depend on the nature of that use and how they have used our controls. Any person can see each of the specific interests we maintain about them for advertising by visiting Ads Preferences, which lets people see what interests we use to choose ads for them—and to edit or delete these interests. We also provide more detailed information about how we use data to decide what ads to show to people in our "About Facebook Ads" page, at https://www.facebook.com/ads/about. And, we do not sell people's information to anyone, and we never will.

All users must expressly consent to Facebook's Terms and Data Policy when registering for Facebook. The Data Policy explains the kinds of information we collect, how we use this information, how we share this information, and how users can manage and delete information.

Facebook does not create profiles for people without a Facebook account, but we do receive some information from devices and browsers that may be used by non-users. For example:

- When people visit apps or websites that feature our technologies—like the Facebook Like or Comment button—our servers automatically log (i) standard browser or app records of the fact that a particular device or user visited the website or app (this connection to Facebook's servers occurs automatically when a person visits a website or app that contains our technologies, such as a Like button, and is an inherent function of Internet design); and (ii) any additional information the publisher of the app or website chooses to share with Facebook about the person's activities on that site (such as the fact that a purchase was made on the site). This is a standard feature of the Internet, and most websites and apps share this same information with multiple different third-parties whenever people visit their website or app. When the person visiting a website featuring Facebook's tools is not a registered Facebook user, Facebook does not have information identifying that individual, and it does not create profiles for this individual.

- We also may receive information about the device of a non-registered user if that user visits a part of Facebook that does not require people to log in—such as a public Facebook Page. The information we log when people visit our websites or apps is the same as described above and is the same information that any provider of an online service would receive.

- In addition, Facebook may receive some basic information about devices where Facebook apps are installed, including before people using those devices have registered for Facebook (such as when a user downloads a Facebook app, but has not yet created an account, or if the app is preloaded on a given device). This device data includes things like device model, operating system, IP address, app version and device identifiers. We use this information to provide the right version of the app, help people who want to create accounts (for example, optimizing the registration flow for the specific device),

retrieving bug fixes and measuring and improving app performance. We do not use this information to build profiles about non-registered users.

81. How can you assure us that this won't happen again?

Facebook's policies regarding third-party usage of its platform technologies have prohibited—and continue to prohibit—third-party app developers from selling or licensing user data obtained from Facebook and from sharing any user data obtained from Facebook with any ad network, data broker or other advertising or monetization-related service.

We use a variety of tools to enforce Facebook policies against violating parties, including developers. We review tens of thousands of apps per year and regularly disapprove noncompliant apps as part of our proactive review process. We also use tools like cease and desist letters, account suspensions, letter agreements, and civil litigation. For example, since 2006, Facebook has sent over 1,150 cease-and-desist letters to over 1,600 targets. In 2017, we took action against about 370,000 apps, ranging from imposing certain restrictions to removal of the app from the platform. Moreover, we have required parties who have procured our data without authorization to delete that data. We have invested significant resources in these efforts.

Recently, we announced a number of additional steps we're taking to address concerns raised by Kogan's app.

- **Review our platform.** We will investigate all apps that had access to large amounts of data before the platform changes we announced in 2014, and we will audit any app where we identify suspicious activity. If we identify misuses of data, we'll take immediate action, including banning the app from our platform and pursuing legal action if appropriate.

- **Tell people about data misuse.** We will tell people about apps that have misused their data. This includes building a way for people to know if their data might have been accessed via the app. Moving forward, if we remove an app, we will tell people.

- **Turn off access for unused apps.** If someone has not used an app within the last three months, we will turn off the app's access to their data.

- **Restrict Facebook Login data.** We are changing Login, so that the only data that an app can request without app review will include name, profile photo, and email address. Requesting any other data will require approval from Facebook. We will also no longer allow apps to ask for access to information like religious or political views, relationship status and details, custom friends lists, education and work history, fitness activity, book reading and music listening activity, news reading, video watch activity, and games activity. We will encourage people to manage the apps they use. We already show people what apps their accounts are connected to and allow them to control what data they've permitted those apps to use. But we're making it easier for people to see what apps they use and the information they have shared with those apps.

- **Reward people who find vulnerabilities.** We launched the Data Abuse Bounty program so that people can report to us any misuses of data by app developers.

- **Update our policies.** We have updated our terms and Data Policy to explain how we use data and how data is shared with app developers.

82. What do you have in place to prevent this again, negate its damage now, and punish ALL perpetrators?

Facebook's policies regarding third-party usage of its platform technologies have prohibited—and continue to prohibit—third-party app developers from selling or licensing user data obtained from Facebook and from sharing any user data obtained from Facebook with any ad network, data broker or other advertising or monetization-related service.

We use a variety of tools to enforce Facebook policies against violating parties, including developers. We review tens of thousands of apps per year and regularly disapprove noncompliant apps as part of our proactive review process. We also use tools like cease and desist letters, account suspensions, letter agreements, and civil litigation. For example, since 2006, Facebook has sent over 1,150 cease-and-desist letters to over 1,600 targets. In 2017, we took action against about 370,000 apps, ranging from imposing certain restrictions to removal of the app from the platform. Moreover, we have required parties who have procured our data without authorization to delete that data. We have invested significant resources in these efforts.

Recently, we announced a number of additional steps we're taking to address concerns raised by Kogan's app.

- **Review our platform.** We will investigate all apps that had access to large amounts of data before the platform changes we announced in 2014, and we will audit any app where we identify suspicious activity. If we identify misuses of data, we'll take immediate action, including banning the app from our platform and pursuing legal action if appropriate.

- **Tell people about data misuse.** We will tell people about apps that have misused their data. This includes building a way for people to know if their data might have been accessed via the app. Moving forward, if we remove an app, we will tell people.

- **Turn off access for unused apps.** If someone has not used an app within the last three months, we will turn off the app's access to their data.

- **Restrict Facebook Login data.** We are changing Login, so that the only data that an app can request without app review will include name, profile photo, and email address. Requesting any other data will require approval from Facebook. We will also no longer allow apps to ask for access to information like religious or political views, relationship status and details, custom friends lists, education and work history, fitness activity, book reading and music listening activity, news reading, video watch activity, and games activity. We will encourage people to manage the apps they use. We already show people what apps their accounts are connected to and allow them to

control what data they've permitted those apps to use. But we're making it easier for people to see what apps they use and the information they have shared with those apps.

- **Reward people who find vulnerabilities.** We launched the Data Abuse Bounty program so that people can report to us any misuses of data by app developers.

- **Update our policies.** We have updated our terms and Data Policy to explain how we use data and how data is shared with app developers.

83. What definitive actions will you take to protect the individual's right to keep data private?

We believe everyone deserves good privacy controls. A user owns the information they share on Facebook. This means they decide what they share and who they share it with on Facebook, and they can change their mind. We require websites and apps who use our tools to tell users they're collecting and sharing their information with us, and to get users' permission to do so.

Everyone has the right to expect strong protections for their information. We also need to do our part to help keep our community safe, in a way that's consistent with people's privacy expectations. We've recently announced several steps to give people more control over their privacy, including a new Privacy Shortcuts tool that we're rolling out now to give people information about how to control their information, including choosing who can see what they post and adding protections like two-factor authentication to their account. People can learn more about how to protect their privacy in our updated Data Policy and in our Privacy Basics feature (https://www.facebook.com/about/basics).

We are in the process of investigating every app that had access to a large amount of information before we changed our Platform in 2014. The investigation process is in full swing. We have large teams of internal and external experts working hard to investigate these apps as quickly as possible. As of early June 2018, thousands of apps have been investigated and around 200 apps have been suspended—pending a thorough investigation into whether they did in fact misuse any data. Where we find evidence that these or other apps did misuse data, we will ban them and let people know.

Facebook is generally not opposed to regulation but wants to ensure it is the right regulation. The issues facing the industry are complex, multi-faceted, and affect an important part of peoples' lives. As such, Facebook is absolutely committed to working with regulators, like Congress, to craft the right regulations. Facebook would be happy to review any proposed legislation and provide comments.

84. Will you provide users the guaranteed option to I) download a copy of ALL data you have acquired on them and 2) allow and guarantee EVERY past and present user can have ALL their data deleted from ALL servers and ALL archives?

We believe everyone deserves good privacy controls. A user owns the information they share on Facebook. This means they decide what they share and who they share it with on

Facebook, and they can change their mind. We require websites and apps who use our tools to tell users they're collecting and sharing their information with us, and to get users' permission to do so.

Everyone has the right to expect strong protections for their information. We also need to do our part to help keep our community safe, in a way that's consistent with people's privacy expectations. We've recently announced several steps to give people more control over their privacy, including a new Privacy Shortcuts tool that we're rolling out now to give people information about how to control their information, including choosing who can see what they post and adding protections like two-factor authentication to their account. People can learn more about how to protect their privacy in our updated Data Policy and in our Privacy Basics feature (https://www.facebook.com/about/basics).

We are in the process of investigating every app that had access to a large amount of information before we changed our Platform in 2014. The investigation process is in full swing. We have large teams of internal and external experts working hard to investigate these apps as quickly as possible. As of early June 2018, thousands of apps have been investigated and around 200 apps have been suspended—pending a thorough investigation into whether they did in fact misuse any data. Where we find evidence that these or other apps did misuse data, we will ban them and let people know.

Facebook is generally not opposed to regulation but wants to ensure it is the right regulation. The issues facing the industry are complex, multi-faceted, and affect an important part of peoples' lives. As such, Facebook is absolutely committed to working with regulators, like Congress, to craft the right regulations. Facebook would be happy to review any proposed legislation and provide comments.

85. How can you keep this from happening again?

Facebook's policies regarding third-party usage of its platform technologies have prohibited—and continue to prohibit—third-party app developers from selling or licensing user data obtained from Facebook and from sharing any user data obtained from Facebook with any ad network, data broker or other advertising or monetization-related service.

We use a variety of tools to enforce Facebook policies against violating parties, including developers. We review tens of thousands of apps per year and regularly disapprove noncompliant apps as part of our proactive review process. We also use tools like cease and desist letters, account suspensions, letter agreements, and civil litigation. For example, since 2006, Facebook has sent over 1,150 cease-and-desist letters to over 1,600 targets. In 2017, we took action against about 370,000 apps, ranging from imposing certain restrictions to removal of the app from the platform. Moreover, we have required parties who have procured our data without authorization to delete that data. We have invested significant resources in these efforts.

Recently, we announced a number of additional steps we're taking to address concerns raised by Kogan's app.

- **Review our platform.** We will investigate all apps that had access to large amounts of data before the platform changes we announced in 2014, and we will audit any app where we identify suspicious activity. If we identify misuses of data, we'll take immediate action, including banning the app from our platform and pursuing legal action if appropriate.

- **Tell people about data misuse.** We will tell people about apps that have misused their data. This includes building a way for people to know if their data might have been accessed via the app. Moving forward, if we remove an app, we will tell people.

- **Turn off access for unused apps.** If someone has not used an app within the last three months, we will turn off the app's access to their data.

- **Restrict Facebook Login data.** We are changing Login, so that the only data that an app can request without app review will include name, profile photo, and email address. Requesting any other data will require approval from Facebook. We will also no longer allow apps to ask for access to information like religious or political views, relationship status and details, custom friends lists, education and work history, fitness activity, book reading and music listening activity, news reading, video watch activity, and games activity. We will encourage people to manage the apps they use. We already show people what apps their accounts are connected to and allow them to control what data they've permitted those apps to use. But we're making it easier for people to see what apps they use and the information they have shared with those apps.

- **Reward people who find vulnerabilities.** We launched the Data Abuse Bounty program so that people can report to us any misuses of data by app developers.

- **Update our policies.** We have updated our terms and Data Policy to explain how we use data and how data is shared with app developers.

86. What will you do to ensure that people's data already released will not be used improperly in the future? What changes will you implement to keep people's data safe moving forward? How will you keep bots from setting up phony accounts? How will Facebook combat the spread of fake news?

Facebook's policies regarding third-party usage of its platform technologies have prohibited—and continue to prohibit—third-party app developers from selling or licensing user data obtained from Facebook and from sharing any user data obtained from Facebook with any ad network, data broker or other advertising or monetization-related service.

We use a variety of tools to enforce Facebook policies against violating parties, including developers. We review tens of thousands of apps per year and regularly disapprove noncompliant apps as part of our proactive review process. We also use tools like cease and desist letters, account suspensions, letter agreements, and civil litigation. For example, since 2006, Facebook has sent over 1,150 cease-and-desist letters to over 1,600 targets. In 2017, we took action against about 370,000 apps, ranging from imposing certain restrictions to removal of the app from the

platform. Moreover, we have required parties who have procured our data without authorization to delete that data. We have invested significant resources in these efforts.

Recently, we announced a number of additional steps we're taking to address concerns raised by Kogan's app.

- **Review our platform.** We will investigate all apps that had access to large amounts of data before the platform changes we announced in 2014, and we will audit any app where we identify suspicious activity. If we identify misuses of data, we'll take immediate action, including banning the app from our platform and pursuing legal action if appropriate.

- **Tell people about data misuse.** We will tell people about apps that have misused their data. This includes building a way for people to know if their data might have been accessed via the app. Moving forward, if we remove an app, we will tell people.

- **Turn off access for unused apps.** If someone has not used an app within the last three months, we will turn off the app's access to their data.

- **Restrict Facebook Login data.** We are changing Login, so that the only data that an app can request without app review will include name, profile photo, and email address. Requesting any other data will require approval from Facebook. We will also no longer allow apps to ask for access to information like religious or political views, relationship status and details, custom friends lists, education and work history, fitness activity, book reading and music listening activity, news reading, video watch activity, and games activity. We will encourage people to manage the apps they use. We already show people what apps their accounts are connected to and allow them to control what data they've permitted those apps to use. But we're making it easier for people to see what apps they use and the information they have shared with those apps.

- **Reward people who find vulnerabilities.** We launched the Data Abuse Bounty program so that people can report to us any misuses of data by app developers.

- **Update our policies.** We have updated our terms and Data Policy to explain how we use data and how data is shared with app developers.

87. What are you planning to do for the people whose personal data was stolen?

Facebook's policies regarding third-party usage of its platform technologies have prohibited—and continue to prohibit—third-party app developers from selling or licensing user data obtained from Facebook and from sharing any user data obtained from Facebook with any ad network, data broker or other advertising or monetization-related service.

We use a variety of tools to enforce Facebook policies against violating parties, including developers. We review tens of thousands of apps per year and regularly disapprove noncompliant apps as part of our proactive review process. We also use tools like cease and desist letters,

account suspensions, letter agreements, and civil litigation. For example, since 2006, Facebook has sent over 1,150 cease-and-desist letters to over 1,600 targets. In 2017, we took action against about 370,000 apps, ranging from imposing certain restrictions to removal of the app from the platform. Moreover, we have required parties who have procured our data without authorization to delete that data. We have invested significant resources in these efforts.

Recently, we announced a number of additional steps we're taking to address concerns raised by Kogan's app.

- **Review our platform.** We will investigate all apps that had access to large amounts of data before the platform changes we announced in 2014, and we will audit any app where we identify suspicious activity. If we identify misuses of data, we'll take immediate action, including banning the app from our platform and pursuing legal action if appropriate.

- **Tell people about data misuse.** We will tell people about apps that have misused their data. This includes building a way for people to know if their data might have been accessed via the app. Moving forward, if we remove an app, we will tell people.

- **Turn off access for unused apps.** If someone has not used an app within the last three months, we will turn off the app's access to their data.

- **Restrict Facebook Login data.** We are changing Login, so that the only data that an app can request without app review will include name, profile photo, and email address. Requesting any other data will require approval from Facebook. We will also no longer allow apps to ask for access to information like religious or political views, relationship status and details, custom friends lists, education and work history, fitness activity, book reading and music listening activity, news reading, video watch activity, and games activity. We will encourage people to manage the apps they use. We already show people what apps their accounts are connected to and allow them to control what data they've permitted those apps to use. But we're making it easier for people to see what apps they use and the information they have shared with those apps.

- **Reward people who find vulnerabilities.** We launched the Data Abuse Bounty program so that people can report to us any misuses of data by app developers.

- **Update our policies.** We have updated our terms and Data Policy to explain how we use data and how data is shared with app developers.

88. To regain public trust, could FB allow individuals to opt-out of ALL ad targeting?

To build a secure product with extensive infrastructure that connects people wherever they live or whatever their income level, we need to make sure everyone can afford it. Advertising lets us keep Facebook free, which ensures it remains affordable for everyone. We also believe the ads you see across the Facebook family of apps and services should be useful and relevant to you. Users can't opt out of seeing ads altogether because selling ads is what

keeps Facebook free, but they do have different options to control how their data can and can't be used to show them ads. They're all found in ad preferences, which allows users to turn off the use of all data collected from partners off Facebook to target ads. Users can also decide which of their profile fields they want used for ad targeting in the Information section under "About you." Users can remove themselves from interests under "Your interests" and categories under "Your categories." And, we do not sell people's information to anyone, and we never will.

Facebook is committed to transparency for all ads, including ads with political content. Facebook believes that people should be able to easily understand why they are seeing ads, who paid for them, and what other ads those advertisers are running. As such, Facebook only allows authorized advertisers to run ads about elections or issues that are being debated across the country. In order to be authorized by Facebook, advertisers will need to confirm their identity and location. Furthermore, all political and issue ads will include a disclosure which reads: "Paid for by," and when users click on this disclosure they will be able to see details about the advertiser. Users will also be able to see an explanation of why they saw the particular ad. This is similar to the disclosure included on political TV advertisements. We just launched globally View Active Ads, a feature that will enable anyone to see all of the ads an advertiser is currently running by visiting the advertiser's Facebook Page.

89. What measures were taken to prevent malicious third parties to gain access to the info leaked?

We believe everyone deserves good privacy controls. A user owns the information they share on Facebook. This means they decide what they share and who they share it with on Facebook, and they can change their mind. We require websites and apps who use our tools to tell users they're collecting and sharing their information with us, and to get users' permission to do so.

Everyone has the right to expect strong protections for their information. We also need to do our part to help keep our community safe, in a way that's consistent with people's privacy expectations. We've recently announced several steps to give people more control over their privacy, including a new Privacy Shortcuts tool that we're rolling out now to give people information about how to control their information, including choosing who can see what they post and adding protections like two-factor authentication to their account. People can learn more about how to protect their privacy in our updated Data Policy and in our Privacy Basics feature (https://www.facebook.com/about/basics).

We are in the process of investigating every app that had access to a large amount of information before we changed our Platform in 2014. The investigation process is in full swing. We have large teams of internal and external experts working hard to investigate these apps as quickly as possible. As of early June 2018, thousands of apps have been investigated and around 200 apps have been suspended—pending a thorough investigation into whether they did in fact misuse any data. Where we find evidence that these or other apps did misuse data, we will ban them and let people know.

Facebook is generally not opposed to regulation but wants to ensure it is the right regulation. The issues facing the industry are complex, multi-faceted, and affect an important

part of peoples' lives. As such, Facebook is absolutely committed to working with regulators, like Congress, to craft the right regulations. Facebook would be happy to review any proposed legislation and provide comments.

90. Can you imagine centrally sourcing and tracking/tracing all usage of Facebook data by third parties?

We believe that it's important to communicate with people about the information that we collect and how people can control it. As explained in our Data Policy, we collect three basic categories of data about people:

(1) data about things people do and share (and who they connect with) on our services;

(2) data about the devices people use to access our services; and

(3) data we receive from partners, including the websites and apps that use our business tools.

We collect information about the people, Pages, accounts, hashtags, and groups users are connected to and how they interact with them across our Products, such as people a user communicates with the most or groups users are part of. We also collect contact information if they choose to upload, sync, or import it from a device (such as an address book or call log or SMS log history), which we use for things like helping them and others find people they may know.

The data we use to show ads to people depends on the data we have received from people. For people who are new to Facebook, we may have minimal data that we can use. For people who have used our services for longer, we likely have more data, but the amount of data will depend on the nature of that use and how they have used our controls. Any person can see each of the specific interests we maintain about them for advertising by visiting Ads Preferences, which lets people see what interests we use to choose ads for them—and to edit or delete these interests. We also provide more detailed information about how we use data to decide what ads to show to people in our "About Facebook Ads" page, at https://www.facebook.com/ads/about. And, we do not sell people's information to anyone, and we never will.

All users must expressly consent to Facebook's Terms and Data Policy when registering for Facebook. The Data Policy explains the kinds of information we collect, how we use this information, how we share this information, and how users can manage and delete information.

Facebook does not create profiles for people without a Facebook account, but we do receive some information from devices and browsers that may be used by non-users. For example:

- When people visit apps or websites that feature our technologies—like the Facebook Like or Comment button—our servers automatically log (i) standard browser or app records of the fact that a particular device or user visited the website or app (this connection to Facebook's servers occurs automatically when a person visits a website or app that

contains our technologies, such as a Like button, and is an inherent function of Internet design); and (ii) any additional information the publisher of the app or website chooses to share with Facebook about the person's activities on that site (such as the fact that a purchase was made on the site). This is a standard feature of the Internet, and most websites and apps share this same information with multiple different third-parties whenever people visit their website or app. When the person visiting a website featuring Facebook's tools is not a registered Facebook user, Facebook does not have information identifying that individual, and it does not create profiles for this individual.

- We also may receive information about the device of a non-registered user if that user visits a part of Facebook that does not require people to log in—such as a public Facebook Page. The information we log when people visit our websites or apps is the same as described above and is the same information that any provider of an online service would receive.

- In addition, Facebook may receive some basic information about devices where Facebook apps are installed, including before people using those devices have registered for Facebook (such as when a user downloads a Facebook app, but has not yet created an account, or if the app is preloaded on a given device). This device data includes things like device model, operating system, IP address, app version and device identifiers. We use this information to provide the right version of the app, help people who want to create accounts (for example, optimizing the registration flow for the specific device), retrieving bug fixes and measuring and improving app performance. We do not use this information to build profiles about non-registered users.

91. If he's required to break off some of his company, what components would he spin off?

As discussed with your staff, this question is not germane to the hearing.

92. What are you doing to restore public faith and keep Facebook as safe as possible?

Facebook's policies regarding third-party usage of its platform technologies have prohibited—and continue to prohibit—third-party app developers from selling or licensing user data obtained from Facebook and from sharing any user data obtained from Facebook with any ad network, data broker or other advertising or monetization-related service.

We use a variety of tools to enforce Facebook policies against violating parties, including developers. We review tens of thousands of apps per year and regularly disapprove noncompliant apps as part of our proactive review process. We also use tools like cease and desist letters, account suspensions, letter agreements, and civil litigation. For example, since 2006, Facebook has sent over 1,150 cease-and-desist letters to over 1,600 targets. In 2017, we took action against about 370,000 apps, ranging from imposing certain restrictions to removal of the app from the platform. Moreover, we have required parties who have procured our data without authorization to delete that data. We have invested significant resources in these efforts.

Recently, we announced a number of additional steps we're taking to address concerns raised by Kogan's app.

- **Review our platform.** We will investigate all apps that had access to large amounts of data before the platform changes we announced in 2014, and we will audit any app where we identify suspicious activity. If we identify misuses of data, we'll take immediate action, including banning the app from our platform and pursuing legal action if appropriate.

- **Tell people about data misuse.** We will tell people about apps that have misused their data. This includes building a way for people to know if their data might have been accessed via the app. Moving forward, if we remove an app, we will tell people.

- **Turn off access for unused apps.** If someone has not used an app within the last three months, we will turn off the app's access to their data.

- **Restrict Facebook Login data.** We are changing Login, so that the only data that an app can request without app review will include name, profile photo, and email address. Requesting any other data will require approval from Facebook. We will also no longer allow apps to ask for access to information like religious or political views, relationship status and details, custom friends lists, education and work history, fitness activity, book reading and music listening activity, news reading, video watch activity, and games activity. We will encourage people to manage the apps they use. We already show people what apps their accounts are connected to and allow them to control what data they've permitted those apps to use. But we're making it easier for people to see what apps they use and the information they have shared with those apps.

- **Reward people who find vulnerabilities.** We launched the Data Abuse Bounty program so that people can report to us any misuses of data by app developers.

- **Update our policies.** We have updated our terms and Data Policy to explain how we use data and how data is shared with app developers.

93. What steps are you taking to ensure that this does not happen again?

Facebook's policies regarding third-party usage of its platform technologies have prohibited—and continue to prohibit—third-party app developers from selling or licensing user data obtained from Facebook and from sharing any user data obtained from Facebook with any ad network, data broker or other advertising or monetization-related service.

We use a variety of tools to enforce Facebook policies against violating parties, including developers. We review tens of thousands of apps per year and regularly disapprove noncompliant apps as part of our proactive review process. We also use tools like cease and desist letters, account suspensions, letter agreements, and civil litigation. For example, since 2006, Facebook has sent over 1,150 cease-and-desist letters to over 1,600 targets. In 2017, we took action against about 370,000 apps, ranging from imposing certain restrictions to removal of the app from the

platform. Moreover, we have required parties who have procured our data without authorization to delete that data. We have invested significant resources in these efforts.

Recently, we announced a number of additional steps we're taking to address concerns raised by Kogan's app.

- **Review our platform.** We will investigate all apps that had access to large amounts of data before the platform changes we announced in 2014, and we will audit any app where we identify suspicious activity. If we identify misuses of data, we'll take immediate action, including banning the app from our platform and pursuing legal action if appropriate.

- **Tell people about data misuse.** We will tell people about apps that have misused their data. This includes building a way for people to know if their data might have been accessed via the app. Moving forward, if we remove an app, we will tell people.

- **Turn off access for unused apps.** If someone has not used an app within the last three months, we will turn off the app's access to their data.

- **Restrict Facebook Login data.** We are changing Login, so that the only data that an app can request without app review will include name, profile photo, and email address. Requesting any other data will require approval from Facebook. We will also no longer allow apps to ask for access to information like religious or political views, relationship status and details, custom friends lists, education and work history, fitness activity, book reading and music listening activity, news reading, video watch activity, and games activity. We will encourage people to manage the apps they use. We already show people what apps their accounts are connected to and allow them to control what data they've permitted those apps to use. But we're making it easier for people to see what apps they use and the information they have shared with those apps.

- **Reward people who find vulnerabilities.** We launched the Data Abuse Bounty program so that people can report to us any misuses of data by app developers.

- **Update our policies.** We have updated our terms and Data Policy to explain how we use data and how data is shared with app developers.

94. I would ask Mr. Zuckerberg what guarantee can he give his users that Facebook will treat our personal information and data the way he would like his to be treated.

We believe everyone deserves good privacy controls. A user owns the information they share on Facebook. This means they decide what they share and who they share it with on Facebook, and they can change their mind. We require websites and apps who use our tools to tell users they're collecting and sharing their information with us, and to get users' permission to do so.

Everyone has the right to expect strong protections for their information. We also need to do our part to help keep our community safe, in a way that's consistent with people's privacy expectations. We've recently announced several steps to give people more control over their privacy, including a new Privacy Shortcuts tool that we're rolling out now to give people information about how to control their information, including choosing who can see what they post and adding protections like two-factor authentication to their account. People can learn more about how to protect their privacy in our updated Data Policy and in our Privacy Basics feature (https://www.facebook.com/about/basics).

We are in the process of investigating every app that had access to a large amount of information before we changed our Platform in 2014. The investigation process is in full swing. We have large teams of internal and external experts working hard to investigate these apps as quickly as possible. As of early June 2018, thousands of apps have been investigated and around 200 apps have been suspended—pending a thorough investigation into whether they did in fact misuse any data. Where we find evidence that these or other apps did misuse data, we will ban them and let people know.

Facebook is generally not opposed to regulation but wants to ensure it is the right regulation. The issues facing the industry are complex, multi-faceted, and affect an important part of peoples' lives. As such, Facebook is absolutely committed to working with regulators, like Congress, to craft the right regulations. Facebook would be happy to review any proposed legislation and provide comments.

95. What will Mark and Facebook do in the future to protect Facebook users' privacy?

We believe everyone deserves good privacy controls. A user owns the information they share on Facebook. This means they decide what they share and who they share it with on Facebook, and they can change their mind. We require websites and apps who use our tools to tell users they're collecting and sharing their information with us, and to get users' permission to do so.

Everyone has the right to expect strong protections for their information. We also need to do our part to help keep our community safe, in a way that's consistent with people's privacy expectations. We've recently announced several steps to give people more control over their privacy, including a new Privacy Shortcuts tool that we're rolling out now to give people information about how to control their information, including choosing who can see what they post and adding protections like two-factor authentication to their account. People can learn more about how to protect their privacy in our updated Data Policy and in our Privacy Basics feature (https://www.facebook.com/about/basics).

We are in the process of investigating every app that had access to a large amount of information before we changed our Platform in 2014. The investigation process is in full swing. We have large teams of internal and external experts working hard to investigate these apps as quickly as possible. As of early June 2018, thousands of apps have been investigated and around 200 apps have been suspended—pending a thorough investigation into whether they did in fact misuse any data. Where we find evidence that these or other apps did misuse data, we will ban them and let people know.

Facebook is generally not opposed to regulation but wants to ensure it is the right regulation. The issues facing the industry are complex, multi-faceted, and affect an important part of peoples' lives. As such, Facebook is absolutely committed to working with regulators, like Congress, to craft the right regulations. Facebook would be happy to review any proposed legislation and provide comments.

96. How can you change your business model to protect the personal information of your Facebook members while maintaining your marketing sales?

To build a secure product with extensive infrastructure that connects people wherever they live or whatever their income level, we need to make sure everyone can afford it. Advertising lets us keep Facebook free, which ensures it remains affordable for everyone. We also believe the ads you see across the Facebook family of apps and services should be useful and relevant to you. Users can't opt out of seeing ads altogether because selling ads is what keeps Facebook free, but they do have different options to control how their data can and can't be used to show them ads. They're all found in ad preferences, which allows users to turn off the use of all data collected from partners off Facebook to target ads. Users can also decide which of their profile fields they want used for ad targeting in the Information section under "About you." Users can remove themselves from interests under "Your interests" and categories under "Your categories." And, we do not sell people's information to anyone, and we never will.

Facebook is committed to transparency for all ads, including ads with political content. Facebook believes that people should be able to easily understand why they are seeing ads, who paid for them, and what other ads those advertisers are running. As such, Facebook only allows authorized advertisers to run ads about elections or issues that are being debated across the country. In order to be authorized by Facebook, advertisers will need to confirm their identity and location. Furthermore, all political and issue ads will include a disclosure which reads: "Paid for by," and when users click on this disclosure they will be able to see details about the advertiser. Users will also be able to see an explanation of why they saw the particular ad. This is similar to the disclosure included on political TV advertisements. We just launched globally View Active Ads, a feature that will enable anyone to see all of the ads an advertiser is currently running by visiting the advertiser's Facebook Page.

97. FB failed to protect its users' private data. How will FB make it up to its users?

We believe everyone deserves good privacy controls. A user owns the information they share on Facebook. This means they decide what they share and who they share it with on Facebook, and they can change their mind. We require websites and apps who use our tools to tell users they're collecting and sharing their information with us, and to get users' permission to do so.

Everyone has the right to expect strong protections for their information. We also need to do our part to help keep our community safe, in a way that's consistent with people's privacy expectations. We've recently announced several steps to give people more control over their privacy, including a new Privacy Shortcuts tool that we're rolling out now to give people information about how to control their information, including choosing who can see what they post and adding protections like two-factor authentication to their account. People can learn more

about how to protect their privacy in our updated Data Policy and in our Privacy Basics feature (https://www.facebook.com/about/basics).

We are in the process of investigating every app that had access to a large amount of information before we changed our Platform in 2014. The investigation process is in full swing. We have large teams of internal and external experts working hard to investigate these apps as quickly as possible. As of early June 2018, thousands of apps have been investigated and around 200 apps have been suspended—pending a thorough investigation into whether they did in fact misuse any data. Where we find evidence that these or other apps did misuse data, we will ban them and let people know.

Facebook is generally not opposed to regulation but wants to ensure it is the right regulation. The issues facing the industry are complex, multi-faceted, and affect an important part of peoples' lives. As such, Facebook is absolutely committed to working with regulators, like Congress, to craft the right regulations. Facebook would be happy to review any proposed legislation and provide comments.

98. What will Facebook do now to assure that our data will not be misused?

We believe everyone deserves good privacy controls. A user owns the information they share on Facebook. This means they decide what they share and who they share it with on Facebook, and they can change their mind. We require websites and apps who use our tools to tell users they're collecting and sharing their information with us, and to get users' permission to do so.

Everyone has the right to expect strong protections for their information. We also need to do our part to help keep our community safe, in a way that's consistent with people's privacy expectations. We've recently announced several steps to give people more control over their privacy, including a new Privacy Shortcuts tool that we're rolling out now to give people information about how to control their information, including choosing who can see what they post and adding protections like two-factor authentication to their account. People can learn more about how to protect their privacy in our updated Data Policy and in our Privacy Basics feature (https://www.facebook.com/about/basics).

We are in the process of investigating every app that had access to a large amount of information before we changed our Platform in 2014. The investigation process is in full swing. We have large teams of internal and external experts working hard to investigate these apps as quickly as possible. As of early June 2018, thousands of apps have been investigated and around 200 apps have been suspended—pending a thorough investigation into whether they did in fact misuse any data. Where we find evidence that these or other apps did misuse data, we will ban them and let people know.

Facebook is generally not opposed to regulation but wants to ensure it is the right regulation. The issues facing the industry are complex, multi-faceted, and affect an important part of peoples' lives. As such, Facebook is absolutely committed to working with regulators, like Congress, to craft the right regulations. Facebook would be happy to review any proposed legislation and provide comments.

99. How will you ensure equal access and free speech as a gatekeeper to the new public forum?

Freedom of expression is one of our core values, and we believe that adding voices to the conversation creates a richer and more vibrant community. We want people to feel confident that our community welcomes all viewpoints and we are committed to designing our products to give all people a voice and foster the free flow of ideas and culture. We recognize how important it is for Facebook to be a place where people feel empowered to communicate, and we take our role in keeping abuse off our service seriously. Our mission entails embracing diverse views. We err on the side of allowing content, even when some find it objectionable, unless removing that content prevents a specific harm.

However, we are, first and foremost, a technology company. Facebook does not create or edit the content that our users post on our platform. While we seek to be a platform for a broad range of ideas, we do moderate content in good faith according to published community standards in order to keep users on the platform safe, reduce objectionable content and to make sure users participate on the platform responsibly.

100. What, specifically, are you doing to fix this problem?

Facebook's policies regarding third-party usage of its platform technologies have prohibited—and continue to prohibit—third-party app developers from selling or licensing user data obtained from Facebook and from sharing any user data obtained from Facebook with any ad network, data broker or other advertising or monetization-related service.

We use a variety of tools to enforce Facebook policies against violating parties, including developers. We review tens of thousands of apps per year and regularly disapprove noncompliant apps as part of our proactive review process. We also use tools like cease and desist letters, account suspensions, letter agreements, and civil litigation. For example, since 2006, Facebook has sent over 1,150 cease-and-desist letters to over 1,600 targets. In 2017, we took action against about 370,000 apps, ranging from imposing certain restrictions to removal of the app from the platform. Moreover, we have required parties who have procured our data without authorization to delete that data. We have invested significant resources in these efforts.

Recently, we announced a number of additional steps we're taking to address concerns raised by Kogan's app.

- **Review our platform.** We will investigate all apps that had access to large amounts of data before the platform changes we announced in 2014, and we will audit any app where we identify suspicious activity. If we identify misuses of data, we'll take immediate action, including banning the app from our platform and pursuing legal action if appropriate.

- **Tell people about data misuse.** We will tell people about apps that have misused their data. This includes building a way for people to know if their data might have been accessed via the app. Moving forward, if we remove an app, we will tell people.

- **Turn off access for unused apps.** If someone has not used an app within the last three months, we will turn off the app's access to their data.

- **Restrict Facebook Login data.** We are changing Login, so that the only data that an app can request without app review will include name, profile photo, and email address. Requesting any other data will require approval from Facebook. We will also no longer allow apps to ask for access to information like religious or political views, relationship status and details, custom friends lists, education and work history, fitness activity, book reading and music listening activity, news reading, video watch activity, and games activity. We will encourage people to manage the apps they use. We already show people what apps their accounts are connected to and allow them to control what data they've permitted those apps to use. But we're making it easier for people to see what apps they use and the information they have shared with those apps.

- **Reward people who find vulnerabilities.** We launched the Data Abuse Bounty program so that people can report to us any misuses of data by app developers.

- **Update our policies.** We have updated our terms and Data Policy to explain how we use data and how data is shared with app developers.

101. As a matter of policy, does Facebook have allegiance to any nation?

As discussed with your staff, this question is not germane to the hearing.

102. Why can't FB comply with European privacy standards here in US?

As a part of our overall approach to privacy, we are providing the same tools for access, rectification, erasure, data portability and others to people in the US (and globally) that we provide in the European Union under the GDPR. The controls and settings that Facebook is enabling as part of GDPR include settings for controlling our use of face recognition on Facebook and for controlling our ability to use data we collect off Facebook Company Products to target ads. We recently began providing direct notice of these controls and our updated terms to people around the world (including in the US), allowing people to choose whether or not to enable or disable these settings or to consent to our updated terms. Many of these tools (like our Download Your Information tool, ad preferences tool, and Activity Log) have been available globally for many years.

However, the GDPR creates some specific requirements that do not apply in the rest of the world, for example the requirement to provide contact information for the EU Data Protection Officer or to specify legal bases for processing data. We are also looking to be more responsive to regional norms and legal frameworks going forward, and want to have the flexibility to work with local regulators, which is possible with this new model. At the same time, we are changing the provisions in our Facebook, Inc. terms in our user agreements outside the United States to allow people in other countries to file lawsuits against Facebook in their home country, rather than in courts in the US. This transition was part of a continued effort to be locally responsive in countries where people use our services.

103. What are his plans for avoid this in the future?

Facebook's policies regarding third-party usage of its platform technologies have prohibited—and continue to prohibit—third-party app developers from selling or licensing user data obtained from Facebook and from sharing any user data obtained from Facebook with any ad network, data broker or other advertising or monetization-related service.

We use a variety of tools to enforce Facebook policies against violating parties, including developers. We review tens of thousands of apps per year and regularly disapprove noncompliant apps as part of our proactive review process. We also use tools like cease and desist letters, account suspensions, letter agreements, and civil litigation. For example, since 2006, Facebook has sent over 1,150 cease-and-desist letters to over 1,600 targets. In 2017, we took action against about 370,000 apps, ranging from imposing certain restrictions to removal of the app from the platform. Moreover, we have required parties who have procured our data without authorization to delete that data. We have invested significant resources in these efforts.

Recently, we announced a number of additional steps we're taking to address concerns raised by Kogan's app.

- **Review our platform.** We will investigate all apps that had access to large amounts of data before the platform changes we announced in 2014, and we will audit any app where we identify suspicious activity. If we identify misuses of data, we'll take immediate action, including banning the app from our platform and pursuing legal action if appropriate.

- **Tell people about data misuse.** We will tell people about apps that have misused their data. This includes building a way for people to know if their data might have been accessed via the app. Moving forward, if we remove an app, we will tell people.

- **Turn off access for unused apps.** If someone has not used an app within the last three months, we will turn off the app's access to their data.

- **Restrict Facebook Login data.** We are changing Login, so that the only data that an app can request without app review will include name, profile photo, and email address. Requesting any other data will require approval from Facebook. We will also no longer allow apps to ask for access to information like religious or political views, relationship status and details, custom friends lists, education and work history, fitness activity, book reading and music listening activity, news reading, video watch activity, and games activity. We will encourage people to manage the apps they use. We already show people what apps their accounts are connected to and allow them to control what data they've permitted those apps to use. But we're making it easier for people to see what apps they use and the information they have shared with those apps.

- **Reward people who find vulnerabilities.** We launched the Data Abuse Bounty program so that people can report to us any misuses of data by app developers.

- **Update our policies.** We have updated our terms and Data Policy to explain how we use data and how data is shared with app developers.

104. Will you make the security level you apparently personally enjoy available to customers if requested?

We believe everyone deserves good privacy controls. A user owns the information they share on Facebook. This means they decide what they share and who they share it with on Facebook, and they can change their mind. We require websites and apps who use our tools to tell users they're collecting and sharing their information with us, and to get users' permission to do so.

Everyone has the right to expect strong protections for their information. We also need to do our part to help keep our community safe, in a way that's consistent with people's privacy expectations. We've recently announced several steps to give people more control over their privacy, including a new Privacy Shortcuts tool that we're rolling out now to give people information about how to control their information, including choosing who can see what they post and adding protections like two-factor authentication to their account. People can learn more about how to protect their privacy in our updated Data Policy and in our Privacy Basics feature (https://www.facebook.com/about/basics).

We are in the process of investigating every app that had access to a large amount of information before we changed our Platform in 2014. The investigation process is in full swing. We have large teams of internal and external experts working hard to investigate these apps as quickly as possible. As of early June 2018, thousands of apps have been investigated and around 200 apps have been suspended—pending a thorough investigation into whether they did in fact misuse any data. Where we find evidence that these or other apps did misuse data, we will ban them and let people know.

Facebook is generally not opposed to regulation but wants to ensure it is the right regulation. The issues facing the industry are complex, multi-faceted, and affect an important part of peoples' lives. As such, Facebook is absolutely committed to working with regulators, like Congress, to craft the right regulations. Facebook would be happy to review any proposed legislation and provide comments.

105. Since Facebook profited from monetizing users whose privacy and right of privacy has been irrevocably compromised, shouldn't Facebook now compensate those users?

We believe that it's important to communicate with people about the information that we collect and how people can control it. As explained in our Data Policy, we collect three basic categories of data about people:

(1) data about things people do and share (and who they connect with) on our services;

(2) data about the devices people use to access our services; and

(3) data we receive from partners, including the websites and apps that use our business tools.

We collect information about the people, Pages, accounts, hashtags, and groups users are connected to and how they interact with them across our Products, such as people a user communicates with the most or groups users are part of. We also collect contact information if they choose to upload, sync, or import it from a device (such as an address book or call log or SMS log history), which we use for things like helping them and others find people they may know.

The data we use to show ads to people depends on the data we have received from people. For people who are new to Facebook, we may have minimal data that we can use. For people who have used our services for longer, we likely have more data, but the amount of data will depend on the nature of that use and how they have used our controls. Any person can see each of the specific interests we maintain about them for advertising by visiting Ads Preferences, which lets people see what interests we use to choose ads for them—and to edit or delete these interests. We also provide more detailed information about how we use data to decide what ads to show to people in our "About Facebook Ads" page, at https://www.facebook.com/ads/about. And, we do not sell people's information to anyone, and we never will.

All users must expressly consent to Facebook's Terms and Data Policy when registering for Facebook. The Data Policy explains the kinds of information we collect, how we use this information, how we share this information, and how users can manage and delete information.

Facebook does not create profiles for people without a Facebook account, but we do receive some information from devices and browsers that may be used by non-users. For example:

- When people visit apps or websites that feature our technologies—like the Facebook Like or Comment button—our servers automatically log (i) standard browser or app records of the fact that a particular device or user visited the website or app (this connection to Facebook's servers occurs automatically when a person visits a website or app that contains our technologies, such as a Like button, and is an inherent function of Internet design); and (ii) any additional information the publisher of the app or website chooses to share with Facebook about the person's activities on that site (such as the fact that a purchase was made on the site). This is a standard feature of the Internet, and most websites and apps share this same information with multiple different third-parties whenever people visit their website or app. When the person visiting a website featuring Facebook's tools is not a registered Facebook user, Facebook does not have information identifying that individual, and it does not create profiles for this individual.

- We also may receive information about the device of a non-registered user if that user visits a part of Facebook that does not require people to log in—such as a public Facebook Page. The information we log when people visit our websites or apps is the same as described above and is the same information that any provider of an online service would receive.

- In addition, Facebook may receive some basic information about devices where Facebook apps are installed, including before people using those devices have registered for Facebook (such as when a user downloads a Facebook app, but has not yet created an account, or if the app is preloaded on a given device). This device data includes things like device model, operating system, IP address, app version and device identifiers. We use this information to provide the right version of the app, help people who want to create accounts (for example, optimizing the registration flow for the specific device), retrieving bug fixes and measuring and improving app performance. We do not use this information to build profiles about non-registered users.

106. Is there any way to stop Facebook algorithms from collecting users' data?

We believe everyone deserves good privacy controls. A user owns the information they share on Facebook. This means they decide what they share and who they share it with on Facebook, and they can change their mind. We require websites and apps who use our tools to tell users they're collecting and sharing their information with us, and to get users' permission to do so.

Everyone has the right to expect strong protections for their information. We also need to do our part to help keep our community safe, in a way that's consistent with people's privacy expectations. We've recently announced several steps to give people more control over their privacy, including a new Privacy Shortcuts tool that we're rolling out now to give people information about how to control their information, including choosing who can see what they post and adding protections like two-factor authentication to their account. People can learn more about how to protect their privacy in our updated Data Policy and in our Privacy Basics feature (https://www.facebook.com/about/basics).

We are in the process of investigating every app that had access to a large amount of information before we changed our Platform in 2014. The investigation process is in full swing. We have large teams of internal and external experts working hard to investigate these apps as quickly as possible. As of early June 2018, thousands of apps have been investigated and around 200 apps have been suspended—pending a thorough investigation into whether they did in fact misuse any data. Where we find evidence that these or other apps did misuse data, we will ban them and let people know.

Facebook is generally not opposed to regulation but wants to ensure it is the right regulation. The issues facing the industry are complex, multi-faceted, and affect an important part of peoples' lives. As such, Facebook is absolutely committed to working with regulators, like Congress, to craft the right regulations. Facebook would be happy to review any proposed legislation and provide comments.

107. Why should I believe that Facebook's problems with privacy will be resolved this time when they were clearly not adequately resolved when Facebook first had privacy issues exposed several years ago?

We believe everyone deserves good privacy controls. A user owns the information they share on Facebook. This means they decide what they share and who they share it with on

Facebook, and they can change their mind. We require websites and apps who use our tools to tell users they're collecting and sharing their information with us, and to get users' permission to do so.

Everyone has the right to expect strong protections for their information. We also need to do our part to help keep our community safe, in a way that's consistent with people's privacy expectations. We've recently announced several steps to give people more control over their privacy, including a new Privacy Shortcuts tool that we're rolling out now to give people information about how to control their information, including choosing who can see what they post and adding protections like two-factor authentication to their account. People can learn more about how to protect their privacy in our updated Data Policy and in our Privacy Basics feature (https://www.facebook.com/about/basics).

We are in the process of investigating every app that had access to a large amount of information before we changed our Platform in 2014. The investigation process is in full swing. We have large teams of internal and external experts working hard to investigate these apps as quickly as possible. As of early June 2018, thousands of apps have been investigated and around 200 apps have been suspended—pending a thorough investigation into whether they did in fact misuse any data. Where we find evidence that these or other apps did misuse data, we will ban them and let people know.

Facebook is generally not opposed to regulation but wants to ensure it is the right regulation. The issues facing the industry are complex, multi-faceted, and affect an important part of peoples' lives. As such, Facebook is absolutely committed to working with regulators, like Congress, to craft the right regulations. Facebook would be happy to review any proposed legislation and provide comments.

108. Has Facebook ever sold any user data under a data licensing program? If yes to who?

We believe that it's important to communicate with people about the information that we collect and how people can control it. As explained in our Data Policy, we collect three basic categories of data about people:

(1) data about things people do and share (and who they connect with) on our services;

(2) data about the devices people use to access our services; and

(3) data we receive from partners, including the websites and apps that use our business tools.

We collect information about the people, Pages, accounts, hashtags, and groups users are connected to and how they interact with them across our Products, such as people a user communicates with the most or groups users are part of. We also collect contact information if they choose to upload, sync, or import it from a device (such as an address book or call log or SMS log history), which we use for things like helping them and others find people they may know.

The data we use to show ads to people depends on the data we have received from people. For people who are new to Facebook, we may have minimal data that we can use. For people who have used our services for longer, we likely have more data, but the amount of data will depend on the nature of that use and how they have used our controls. Any person can see each of the specific interests we maintain about them for advertising by visiting Ads Preferences, which lets people see what interests we use to choose ads for them—and to edit or delete these interests. We also provide more detailed information about how we use data to decide what ads to show to people in our "About Facebook Ads" page, at https://www.facebook.com/ads/about. And, we do not sell people's information to anyone, and we never will.

All users must expressly consent to Facebook's Terms and Data Policy when registering for Facebook. The Data Policy explains the kinds of information we collect, how we use this information, how we share this information, and how users can manage and delete information.

Facebook does not create profiles for people without a Facebook account, but we do receive some information from devices and browsers that may be used by non-users. For example:

- When people visit apps or websites that feature our technologies—like the Facebook Like or Comment button—our servers automatically log (i) standard browser or app records of the fact that a particular device or user visited the website or app (this connection to Facebook's servers occurs automatically when a person visits a website or app that contains our technologies, such as a Like button, and is an inherent function of Internet design); and (ii) any additional information the publisher of the app or website chooses to share with Facebook about the person's activities on that site (such as the fact that a purchase was made on the site). This is a standard feature of the Internet, and most websites and apps share this same information with multiple different third-parties whenever people visit their website or app. When the person visiting a website featuring Facebook's tools is not a registered Facebook user, Facebook does not have information identifying that individual, and it does not create profiles for this individual.

- We also may receive information about the device of a non-registered user if that user visits a part of Facebook that does not require people to log in—such as a public Facebook Page. The information we log when people visit our websites or apps is the same as described above and is the same information that any provider of an online service would receive.

- In addition, Facebook may receive some basic information about devices where Facebook apps are installed, including before people using those devices have registered for Facebook (such as when a user downloads a Facebook app, but has not yet created an account, or if the app is preloaded on a given device). This device data includes things like device model, operating system, IP address, app version and device identifiers. We use this information to provide the right version of the app, help people who want to create accounts (for example, optimizing the registration flow for the specific device), retrieving bug fixes and measuring and improving app performance. We do not use this information to build profiles about non-registered users.

109. I'm not a Facebook user. When will Facebook & it's entities stop adding unauthorized cookies to my browsers?

We believe that it's important to communicate with people about the information that we collect and how people can control it. As explained in our Data Policy, we collect three basic categories of data about people:

(1) data about things people do and share (and who they connect with) on our services;

(2) data about the devices people use to access our services; and

(3) data we receive from partners, including the websites and apps that use our business tools.

We collect information about the people, Pages, accounts, hashtags, and groups users are connected to and how they interact with them across our Products, such as people a user communicates with the most or groups users are part of. We also collect contact information if they choose to upload, sync, or import it from a device (such as an address book or call log or SMS log history), which we use for things like helping them and others find people they may know.

The data we use to show ads to people depends on the data we have received from people. For people who are new to Facebook, we may have minimal data that we can use. For people who have used our services for longer, we likely have more data, but the amount of data will depend on the nature of that use and how they have used our controls. Any person can see each of the specific interests we maintain about them for advertising by visiting Ads Preferences, which lets people see what interests we use to choose ads for them—and to edit or delete these interests. We also provide more detailed information about how we use data to decide what ads to show to people in our "About Facebook Ads" page, at https://www.facebook.com/ads/about. And, we do not sell people's information to anyone, and we never will.

All users must expressly consent to Facebook's Terms and Data Policy when registering for Facebook. The Data Policy explains the kinds of information we collect, how we use this information, how we share this information, and how users can manage and delete information.

Facebook does not create profiles for people without a Facebook account, but we do receive some information from devices and browsers that may be used by non-users. For example:

- When people visit apps or websites that feature our technologies—like the Facebook Like or Comment button—our servers automatically log (i) standard browser or app records of the fact that a particular device or user visited the website or app (this connection to Facebook's servers occurs automatically when a person visits a website or app that contains our technologies, such as a Like button, and is an inherent function of Internet design); and (ii) any additional information the publisher of the app or website chooses to share with Facebook about the person's activities on that site (such as the fact that a purchase was made on the site). This is a standard feature of the Internet, and most

websites and apps share this same information with multiple different third-parties whenever people visit their website or app. When the person visiting a website featuring Facebook's tools is not a registered Facebook user, Facebook does not have information identifying that individual, and it does not create profiles for this individual.

- We also may receive information about the device of a non-registered user if that user visits a part of Facebook that does not require people to log in—such as a public Facebook Page. The information we log when people visit our websites or apps is the same as described above and is the same information that any provider of an online service would receive.

- In addition, Facebook may receive some basic information about devices where Facebook apps are installed, including before people using those devices have registered for Facebook (such as when a user downloads a Facebook app, but has not yet created an account, or if the app is preloaded on a given device). This device data includes things like device model, operating system, IP address, app version and device identifiers. We use this information to provide the right version of the app, help people who want to create accounts (for example, optimizing the registration flow for the specific device), retrieving bug fixes and measuring and improving app performance. We do not use this information to build profiles about non-registered users.

110. The information button Facebook announced (with source, wiki site, and related articles) is a step in the right direction. Will they offer fact checking services and ratings: notification if an item has been artificially promoted via troll farm and do they have further protections in development such as watermarks or tags too identify video and audio that has been manipulated?

Claiming to be another person violates our Community Standards, and we want to make it harder for anyone to be impersonated on our platform, as well as more effectively detect and deactivate fake accounts to help reduce the spread of spam, false news, and misinformation.

We continually update our technical systems to identify, checkpoint, and remove inauthentic accounts, and we block millions of attempts to register fake accounts every day. As with all security threats, we have been incorporating new insights into our models for detecting fake accounts, including information specific to election issues. We've developed several techniques to help detect and block this type of abuse. At the time someone receives a friend request, our systems are designed to check whether the recipient already has a friend with the same name, along with a variety of other factors that help us determine if an interaction is legitimate. Further, we recently announced new features that use face recognition technology that may help detect when someone is using another user's image as their profile photo—which helps stop impersonation. Users can also report accounts that are impersonating them. This is an area we're continually working to improve so that we can provide a safe and secure experience on Facebook.

111. Will you hold Facebook USA to the same privacy standards as Facebook Europe?

As a part of our overall approach to privacy, we are providing the same tools for access, rectification, erasure, data portability and others to people in the US (and globally) that we provide in the European Union under the GDPR. The controls and settings that Facebook is enabling as part of GDPR include settings for controlling our use of face recognition on Facebook and for controlling our ability to use data we collect off Facebook Company Products to target ads. We recently began providing direct notice of these controls and our updated terms to people around the world (including in the US), allowing people to choose whether or not to enable or disable these settings or to consent to our updated terms. Many of these tools (like our Download Your Information tool, ad preferences tool, and Activity Log) have been available globally for many years.

However, the GDPR creates some specific requirements that do not apply in the rest of the world, for example the requirement to provide contact information for the EU Data Protection Officer or to specify legal bases for processing data. We are also looking to be more responsive to regional norms and legal frameworks going forward, and want to have the flexibility to work with local regulators, which is possible with this new model. At the same time, we are changing the provisions in our Facebook, Inc. terms in our user agreements outside the United States to allow people in other countries to file lawsuits against Facebook in their home country, rather than in courts in the US. This transition was part of a continued effort to be locally responsive in countries where people use our services.

112. What policies will you put in place, and how will you be transparent about data privacy and security, about assuring users that they have full control over all their information?

We believe everyone deserves good privacy controls. A user owns the information they share on Facebook. This means they decide what they share and who they share it with on Facebook, and they can change their mind. We require websites and apps who use our tools to tell users they're collecting and sharing their information with us, and to get users' permission to do so.

Everyone has the right to expect strong protections for their information. We also need to do our part to help keep our community safe, in a way that's consistent with people's privacy expectations. We've recently announced several steps to give people more control over their privacy, including a new Privacy Shortcuts tool that we're rolling out now to give people information about how to control their information, including choosing who can see what they post and adding protections like two-factor authentication to their account. People can learn more about how to protect their privacy in our updated Data Policy and in our Privacy Basics feature (https://www.facebook.com/about/basics).

We are in the process of investigating every app that had access to a large amount of information before we changed our Platform in 2014. The investigation process is in full swing. We have large teams of internal and external experts working hard to investigate these apps as quickly as possible. As of early June 2018, thousands of apps have been investigated and around 200 apps have been suspended—pending a thorough investigation into whether they did in fact misuse any data. Where we find evidence that these or other apps did misuse data, we will ban them and let people know.

Facebook is generally not opposed to regulation but wants to ensure it is the right regulation. The issues facing the industry are complex, multi-faceted, and affect an important part of peoples' lives. As such, Facebook is absolutely committed to working with regulators, like Congress, to craft the right regulations. Facebook would be happy to review any proposed legislation and provide comments.

113. You created a world-wide platform and your social media platform with 2 billion users changed the world. What is Facebook doing to make a positive impact to society?

We believe everyone deserves good privacy controls. A user owns the information they share on Facebook. This means they decide what they share and who they share it with on Facebook, and they can change their mind. We require websites and apps who use our tools to tell users they're collecting and sharing their information with us, and to get users' permission to do so.

Everyone has the right to expect strong protections for their information. We also need to do our part to help keep our community safe, in a way that's consistent with people's privacy expectations. We've recently announced several steps to give people more control over their privacy, including a new Privacy Shortcuts tool that we're rolling out now to give people information about how to control their information, including choosing who can see what they post and adding protections like two-factor authentication to their account. People can learn more about how to protect their privacy in our updated Data Policy and in our Privacy Basics feature (https://www.facebook.com/about/basics).

We are in the process of investigating every app that had access to a large amount of information before we changed our Platform in 2014. The investigation process is in full swing. We have large teams of internal and external experts working hard to investigate these apps as quickly as possible. As of early June 2018, thousands of apps have been investigated and around 200 apps have been suspended—pending a thorough investigation into whether they did in fact misuse any data. Where we find evidence that these or other apps did misuse data, we will ban them and let people know.

Facebook is generally not opposed to regulation but wants to ensure it is the right regulation. The issues facing the industry are complex, multi-faceted, and affect an important part of peoples' lives. As such, Facebook is absolutely committed to working with regulators, like Congress, to craft the right regulations. Facebook would be happy to review any proposed legislation and provide comments.

114. In light of what happened, the misuse of user data, and your platform dependence on the user data as a revenue source, how will Facebook lead the way on data security and privacy? What are your thoughts on how we (in government) should respond to prevent the misuse of user data?

We believe everyone deserves good privacy controls. A user owns the information they share on Facebook. This means they decide what they share and who they share it with on Facebook, and they can change their mind. We require websites and apps who use our tools to

tell users they're collecting and sharing their information with us, and to get users' permission to do so.

Everyone has the right to expect strong protections for their information. We also need to do our part to help keep our community safe, in a way that's consistent with people's privacy expectations. We've recently announced several steps to give people more control over their privacy, including a new Privacy Shortcuts tool that we're rolling out now to give people information about how to control their information, including choosing who can see what they post and adding protections like two-factor authentication to their account. People can learn more about how to protect their privacy in our updated Data Policy and in our Privacy Basics feature (https://www.facebook.com/about/basics).

We are in the process of investigating every app that had access to a large amount of information before we changed our Platform in 2014. The investigation process is in full swing. We have large teams of internal and external experts working hard to investigate these apps as quickly as possible. As of early June 2018, thousands of apps have been investigated and around 200 apps have been suspended—pending a thorough investigation into whether they did in fact misuse any data. Where we find evidence that these or other apps did misuse data, we will ban them and let people know.

Facebook is generally not opposed to regulation but wants to ensure it is the right regulation. The issues facing the industry are complex, multi-faceted, and affect an important part of peoples' lives. As such, Facebook is absolutely committed to working with regulators, like Congress, to craft the right regulations. Facebook would be happy to review any proposed legislation and provide comments.

115. Apple uses a process it calls "differential privacy" to anonymize user data that it aggregates. What is Facebook's process? How can your process provide security and privacy protection for all 2 billion users?

We believe that it's important to communicate with people about the information that we collect and how people can control it. As explained in our Data Policy, we collect three basic categories of data about people:

(1) data about things people do and share (and who they connect with) on our services;

(2) data about the devices people use to access our services; and

(3) data we receive from partners, including the websites and apps that use our business tools.

We collect information about the people, Pages, accounts, hashtags, and groups users are connected to and how they interact with them across our Products, such as people a user communicates with the most or groups users are part of. We also collect contact information if they choose to upload, sync, or import it from a device (such as an address book or call log or SMS log history), which we use for things like helping them and others find people they may know.

The data we use to show ads to people depends on the data we have received from people. For people who are new to Facebook, we may have minimal data that we can use. For people who have used our services for longer, we likely have more data, but the amount of data will depend on the nature of that use and how they have used our controls. Any person can see each of the specific interests we maintain about them for advertising by visiting Ads Preferences, which lets people see what interests we use to choose ads for them—and to edit or delete these interests. We also provide more detailed information about how we use data to decide what ads to show to people in our "About Facebook Ads" page, at https://www.facebook.com/ads/about. And, we do not sell people's information to anyone, and we never will.

All users must expressly consent to Facebook's Terms and Data Policy when registering for Facebook. The Data Policy explains the kinds of information we collect, how we use this information, how we share this information, and how users can manage and delete information.

Facebook does not create profiles for people without a Facebook account, but we do receive some information from devices and browsers that may be used by non-users. For example:

- When people visit apps or websites that feature our technologies—like the Facebook Like or Comment button—our servers automatically log (i) standard browser or app records of the fact that a particular device or user visited the website or app (this connection to Facebook's servers occurs automatically when a person visits a website or app that contains our technologies, such as a Like button, and is an inherent function of Internet design); and (ii) any additional information the publisher of the app or website chooses to share with Facebook about the person's activities on that site (such as the fact that a purchase was made on the site). This is a standard feature of the Internet, and most websites and apps share this same information with multiple different third-parties whenever people visit their website or app. When the person visiting a website featuring Facebook's tools is not a registered Facebook user, Facebook does not have information identifying that individual, and it does not create profiles for this individual.

- We also may receive information about the device of a non-registered user if that user visits a part of Facebook that does not require people to log in—such as a public Facebook Page. The information we log when people visit our websites or apps is the same as described above and is the same information that any provider of an online service would receive.

- In addition, Facebook may receive some basic information about devices where Facebook apps are installed, including before people using those devices have registered for Facebook (such as when a user downloads a Facebook app, but has not yet created an account, or if the app is preloaded on a given device). This device data includes things like device model, operating system, IP address, app version and device identifiers. We use this information to provide the right version of the app, help people who want to create accounts (for example, optimizing the registration flow for the specific device), retrieving bug fixes and measuring and improving app performance. We do not use this information to build profiles about non-registered users.

116. Why not have the end user decide if they want to have their info kept within Facebook?

We believe that it's important to communicate with people about the information that we collect and how people can control it. As explained in our Data Policy, we collect three basic categories of data about people:

(1) data about things people do and share (and who they connect with) on our services;

(2) data about the devices people use to access our services; and

(3) data we receive from partners, including the websites and apps that use our business tools.

We collect information about the people, Pages, accounts, hashtags, and groups users are connected to and how they interact with them across our Products, such as people a user communicates with the most or groups users are part of. We also collect contact information if they choose to upload, sync, or import it from a device (such as an address book or call log or SMS log history), which we use for things like helping them and others find people they may know.

The data we use to show ads to people depends on the data we have received from people. For people who are new to Facebook, we may have minimal data that we can use. For people who have used our services for longer, we likely have more data, but the amount of data will depend on the nature of that use and how they have used our controls. Any person can see each of the specific interests we maintain about them for advertising by visiting Ads Preferences, which lets people see what interests we use to choose ads for them—and to edit or delete these interests. We also provide more detailed information about how we use data to decide what ads to show to people in our "About Facebook Ads" page, at https://www.facebook.com/ads/about. And, we do not sell people's information to anyone, and we never will.

All users must expressly consent to Facebook's Terms and Data Policy when registering for Facebook. The Data Policy explains the kinds of information we collect, how we use this information, how we share this information, and how users can manage and delete information.

Facebook does not create profiles for people without a Facebook account, but we do receive some information from devices and browsers that may be used by non-users. For example:

- When people visit apps or websites that feature our technologies—like the Facebook Like or Comment button—our servers automatically log (i) standard browser or app records of the fact that a particular device or user visited the website or app (this connection to Facebook's servers occurs automatically when a person visits a website or app that contains our technologies, such as a Like button, and is an inherent function of Internet design); and (ii) any additional information the publisher of the app or website chooses to share with Facebook about the person's activities on that site (such as the fact that a purchase was made on the site). This is a standard feature of the Internet, and most

websites and apps share this same information with multiple different third-parties whenever people visit their website or app. When the person visiting a website featuring Facebook's tools is not a registered Facebook user, Facebook does not have information identifying that individual, and it does not create profiles for this individual.

- We also may receive information about the device of a non-registered user if that user visits a part of Facebook that does not require people to log in—such as a public Facebook Page. The information we log when people visit our websites or apps is the same as described above and is the same information that any provider of an online service would receive.

- In addition, Facebook may receive some basic information about devices where Facebook apps are installed, including before people using those devices have registered for Facebook (such as when a user downloads a Facebook app, but has not yet created an account, or if the app is preloaded on a given device). This device data includes things like device model, operating system, IP address, app version and device identifiers. We use this information to provide the right version of the app, help people who want to create accounts (for example, optimizing the registration flow for the specific device), retrieving bug fixes and measuring and improving app performance. We do not use this information to build profiles about non-registered users.

117. How many people on FB had their information compromised by all apps not just Cambridge Analytica?

Facebook's policies regarding third-party usage of its platform technologies have prohibited—and continue to prohibit—third-party app developers from selling or licensing user data accessed from Facebook and from sharing any user data accessed from Facebook with any ad network, data broker or other advertising or monetization-related service. We take action on potential violations of our Platform Policies based on proactive review, external reports, and other signals. Kogan was not permitted to sell or transfer data to third-parties for the purposes he did. In doing so, Kogan and his company violated Facebook's Platform Policies.

On December 11, 2015, *The Guardian* published an article reporting that Kogan and his company, GSR, may have passed information the app had obtained from Facebook users to SCL Elections Ltd. (SCL)/Cambridge Analytica. Facebook immediately banned Kogan's app from our platform and investigated what happened and what further action Facebook should take to enforce our Platform Policies. Facebook considered the matter closed after obtaining written certifications and confirmations from Kogan, GSR, Cambridge Analytica, and SCL declaring that all such data they had obtained was accounted for and destroyed. We did not have any reason to affirmatively question the veracity of any of these certifications until March 2018, when we learned from media reporting that questions had been raised concerning the accuracy of the certifications. Facebook immediately banned Cambridge Analytica and SCL from purchasing advertisements on our services as well as removed the personal accounts of some of their officers. Moreover, while Facebook's policies in place at the time allowed us to audit apps to ensure that they were safe and did not violate its terms, we had already terminated Kogan's app's access to Facebook. Accordingly, there were no ongoing concerns about the level of data that app could access or might access in the future. With the benefit of hindsight, we wish we had

notified people whose information may have been impacted. Facebook has since notified all people potentially impacted with a detailed notice at the top of their News Feed.

118. Why does FB fill your page with ads from sites you visited instead of using info from your friends?

To build a secure product with extensive infrastructure that connects people wherever they live or whatever their income level, we need to make sure everyone can afford it. Advertising lets us keep Facebook free, which ensures it remains affordable for everyone. We also believe the ads you see across the Facebook family of apps and services should be useful and relevant to you. Users can't opt out of seeing ads altogether because selling ads is what keeps Facebook free, but they do have different options to control how their data can and can't be used to show them ads. They're all found in ad preferences, which allows users to turn off the use of all data collected from partners off Facebook to target ads. Users can also decide which of their profile fields they want used for ad targeting in the Information section under "About you." Users can remove themselves from interests under "Your interests" and categories under "Your categories." And, we do not sell people's information to anyone, and we never will.

Facebook is committed to transparency for all ads, including ads with political content. Facebook believes that people should be able to easily understand why they are seeing ads, who paid for them, and what other ads those advertisers are running. As such, Facebook only allows authorized advertisers to run ads about elections or issues that are being debated across the country. In order to be authorized by Facebook, advertisers will need to confirm their identity and location. Furthermore, all political and issue ads will include a disclosure which reads: "Paid for by," and when users click on this disclosure they will be able to see details about the advertiser. Users will also be able to see an explanation of why they saw the particular ad. This is similar to the disclosure included on political TV advertisements. We just launched globally View Active Ads, a feature that will enable anyone to see all of the ads an advertiser is currently running by visiting the advertiser's Facebook Page.

119. What right does Facebook have to freely gather all this private metadata and actual communications of people using its service without notifying how they may be impacted negatively by the company's activities?

We believe that it's important to communicate with people about the information that we collect and how people can control it. As explained in our Data Policy, we collect three basic categories of data about people:

(1) data about things people do and share (and who they connect with) on our services;

(2) data about the devices people use to access our services; and

(3) data we receive from partners, including the websites and apps that use our business tools.

We collect information about the people, Pages, accounts, hashtags, and groups users are connected to and how they interact with them across our Products, such as people a user

communicates with the most or groups users are part of. We also collect contact information if they choose to upload, sync, or import it from a device (such as an address book or call log or SMS log history), which we use for things like helping them and others find people they may know.

The data we use to show ads to people depends on the data we have received from people. For people who are new to Facebook, we may have minimal data that we can use. For people who have used our services for longer, we likely have more data, but the amount of data will depend on the nature of that use and how they have used our controls. Any person can see each of the specific interests we maintain about them for advertising by visiting Ads Preferences, which lets people see what interests we use to choose ads for them—and to edit or delete these interests. We also provide more detailed information about how we use data to decide what ads to show to people in our "About Facebook Ads" page, at https://www.facebook.com/ads/about. And, we do not sell people's information to anyone, and we never will.

All users must expressly consent to Facebook's Terms and Data Policy when registering for Facebook. The Data Policy explains the kinds of information we collect, how we use this information, how we share this information, and how users can manage and delete information.

Facebook does not create profiles for people without a Facebook account, but we do receive some information from devices and browsers that may be used by non-users. For example:

- When people visit apps or websites that feature our technologies—like the Facebook Like or Comment button—our servers automatically log (i) standard browser or app records of the fact that a particular device or user visited the website or app (this connection to Facebook's servers occurs automatically when a person visits a website or app that contains our technologies, such as a Like button, and is an inherent function of Internet design); and (ii) any additional information the publisher of the app or website chooses to share with Facebook about the person's activities on that site (such as the fact that a purchase was made on the site). This is a standard feature of the Internet, and most websites and apps share this same information with multiple different third-parties whenever people visit their website or app. When the person visiting a website featuring Facebook's tools is not a registered Facebook user, Facebook does not have information identifying that individual, and it does not create profiles for this individual.

- We also may receive information about the device of a non-registered user if that user visits a part of Facebook that does not require people to log in—such as a public Facebook Page. The information we log when people visit our websites or apps is the same as described above and is the same information that any provider of an online service would receive.

- In addition, Facebook may receive some basic information about devices where Facebook apps are installed, including before people using those devices have registered for Facebook (such as when a user downloads a Facebook app, but has not yet created an account, or if the app is preloaded on a given device). This device data includes things like device model, operating system, IP address, app version and device identifiers. We

use this information to provide the right version of the app, help people who want to create accounts (for example, optimizing the registration flow for the specific device), retrieving bug fixes and measuring and improving app performance. We do not use this information to build profiles about non-registered users.

120. Should Facebook be regulated by the Federal Government to insure that these abuses do not occur again?

We believe everyone deserves good privacy controls. A user owns the information they share on Facebook. This means they decide what they share and who they share it with on Facebook, and they can change their mind. We require websites and apps who use our tools to tell users they're collecting and sharing their information with us, and to get users' permission to do so.

Everyone has the right to expect strong protections for their information. We also need to do our part to help keep our community safe, in a way that's consistent with people's privacy expectations. We've recently announced several steps to give people more control over their privacy, including a new Privacy Shortcuts tool that we're rolling out now to give people information about how to control their information, including choosing who can see what they post and adding protections like two-factor authentication to their account. People can learn more about how to protect their privacy in our updated Data Policy and in our Privacy Basics feature (https://www.facebook.com/about/basics).

We are in the process of investigating every app that had access to a large amount of information before we changed our Platform in 2014. The investigation process is in full swing. We have large teams of internal and external experts working hard to investigate these apps as quickly as possible. As of early June 2018, thousands of apps have been investigated and around 200 apps have been suspended—pending a thorough investigation into whether they did in fact misuse any data. Where we find evidence that these or other apps did misuse data, we will ban them and let people know.

Facebook is generally not opposed to regulation but wants to ensure it is the right regulation. The issues facing the industry are complex, multi-faceted, and affect an important part of peoples' lives. As such, Facebook is absolutely committed to working with regulators, like Congress, to craft the right regulations. Facebook would be happy to review any proposed legislation and provide comments.

121. Should Facebook be required to disclose all third parties who may be accessing a user's information without the user giving specific permission to such third parties?

We believe that it's important to communicate with people about the information that we collect and how people can control it. As explained in our Data Policy, we collect three basic categories of data about people:

(1) data about things people do and share (and who they connect with) on our services;

(2) data about the devices people use to access our services; and

(3) data we receive from partners, including the websites and apps that use our business tools.

We collect information about the people, Pages, accounts, hashtags, and groups users are connected to and how they interact with them across our Products, such as people a user communicates with the most or groups users are part of. We also collect contact information if they choose to upload, sync, or import it from a device (such as an address book or call log or SMS log history), which we use for things like helping them and others find people they may know.

The data we use to show ads to people depends on the data we have received from people. For people who are new to Facebook, we may have minimal data that we can use. For people who have used our services for longer, we likely have more data, but the amount of data will depend on the nature of that use and how they have used our controls. Any person can see each of the specific interests we maintain about them for advertising by visiting Ads Preferences, which lets people see what interests we use to choose ads for them—and to edit or delete these interests. We also provide more detailed information about how we use data to decide what ads to show to people in our "About Facebook Ads" page, at https://www.facebook.com/ads/about. And, we do not sell people's information to anyone, and we never will.

All users must expressly consent to Facebook's Terms and Data Policy when registering for Facebook. The Data Policy explains the kinds of information we collect, how we use this information, how we share this information, and how users can manage and delete information.

Facebook does not create profiles for people without a Facebook account, but we do receive some information from devices and browsers that may be used by non-users. For example:

- When people visit apps or websites that feature our technologies—like the Facebook Like or Comment button—our servers automatically log (i) standard browser or app records of the fact that a particular device or user visited the website or app (this connection to Facebook's servers occurs automatically when a person visits a website or app that contains our technologies, such as a Like button, and is an inherent function of Internet design); and (ii) any additional information the publisher of the app or website chooses to share with Facebook about the person's activities on that site (such as the fact that a purchase was made on the site). This is a standard feature of the Internet, and most websites and apps share this same information with multiple different third-parties whenever people visit their website or app. When the person visiting a website featuring Facebook's tools is not a registered Facebook user, Facebook does not have information identifying that individual, and it does not create profiles for this individual.

- We also may receive information about the device of a non-registered user if that user visits a part of Facebook that does not require people to log in—such as a public Facebook Page. The information we log when people visit our websites or apps is the same as described above and is the same information that any provider of an online service would receive.

- In addition, Facebook may receive some basic information about devices where Facebook apps are installed, including before people using those devices have registered for Facebook (such as when a user downloads a Facebook app, but has not yet created an account, or if the app is preloaded on a given device). This device data includes things like device model, operating system, IP address, app version and device identifiers. We use this information to provide the right version of the app, help people who want to create accounts (for example, optimizing the registration flow for the specific device), retrieving bug fixes and measuring and improving app performance. We do not use this information to build profiles about non-registered users.

122. Many finance companies are required to obtain annual permission from customers before releasing their information to subsidiaries or other affiliated entities. Why should Facebook not have similar requirements?

We believe that it's important to communicate with people about the information that we collect and how people can control it. As explained in our Data Policy, we collect three basic categories of data about people:

(1) data about things people do and share (and who they connect with) on our services;

(2) data about the devices people use to access our services; and

(3) data we receive from partners, including the websites and apps that use our business tools.

We collect information about the people, Pages, accounts, hashtags, and groups users are connected to and how they interact with them across our Products, such as people a user communicates with the most or groups users are part of. We also collect contact information if they choose to upload, sync, or import it from a device (such as an address book or call log or SMS log history), which we use for things like helping them and others find people they may know.

The data we use to show ads to people depends on the data we have received from people. For people who are new to Facebook, we may have minimal data that we can use. For people who have used our services for longer, we likely have more data, but the amount of data will depend on the nature of that use and how they have used our controls. Any person can see each of the specific interests we maintain about them for advertising by visiting Ads Preferences, which lets people see what interests we use to choose ads for them—and to edit or delete these interests. We also provide more detailed information about how we use data to decide what ads to show to people in our "About Facebook Ads" page, at https://www.facebook.com/ads/about. And, we do not sell people's information to anyone, and we never will.

All users must expressly consent to Facebook's Terms and Data Policy when registering for Facebook. The Data Policy explains the kinds of information we collect, how we use this information, how we share this information, and how users can manage and delete information.

Facebook does not create profiles for people without a Facebook account, but we do receive some information from devices and browsers that may be used by non-users. For example:

- When people visit apps or websites that feature our technologies—like the Facebook Like or Comment button—our servers automatically log (i) standard browser or app records of the fact that a particular device or user visited the website or app (this connection to Facebook's servers occurs automatically when a person visits a website or app that contains our technologies, such as a Like button, and is an inherent function of Internet design); and (ii) any additional information the publisher of the app or website chooses to share with Facebook about the person's activities on that site (such as the fact that a purchase was made on the site). This is a standard feature of the Internet, and most websites and apps share this same information with multiple different third-parties whenever people visit their website or app. When the person visiting a website featuring Facebook's tools is not a registered Facebook user, Facebook does not have information identifying that individual, and it does not create profiles for this individual.

- We also may receive information about the device of a non-registered user if that user visits a part of Facebook that does not require people to log in—such as a public Facebook Page. The information we log when people visit our websites or apps is the same as described above and is the same information that any provider of an online service would receive.

- In addition, Facebook may receive some basic information about devices where Facebook apps are installed, including before people using those devices have registered for Facebook (such as when a user downloads a Facebook app, but has not yet created an account, or if the app is preloaded on a given device). This device data includes things like device model, operating system, IP address, app version and device identifiers. We use this information to provide the right version of the app, help people who want to create accounts (for example, optimizing the registration flow for the specific device), retrieving bug fixes and measuring and improving app performance. We do not use this information to build profiles about non-registered users.

123. Why should the Government now allow Facebook to claim they will fix these abuses of our privacy without the Government being able to monitor and regulate their activities to assure compliance?

We believe everyone deserves good privacy controls. A user owns the information they share on Facebook. This means they decide what they share and who they share it with on Facebook, and they can change their mind. We require websites and apps who use our tools to tell users they're collecting and sharing their information with us, and to get users' permission to do so.

Everyone has the right to expect strong protections for their information. We also need to do our part to help keep our community safe, in a way that's consistent with people's privacy expectations. We've recently announced several steps to give people more control over their privacy, including a new Privacy Shortcuts tool that we're rolling out now to give people

information about how to control their information, including choosing who can see what they post and adding protections like two-factor authentication to their account. People can learn more about how to protect their privacy in our updated Data Policy and in our Privacy Basics feature (https://www.facebook.com/about/basics).

We are in the process of investigating every app that had access to a large amount of information before we changed our Platform in 2014. The investigation process is in full swing. We have large teams of internal and external experts working hard to investigate these apps as quickly as possible. As of early June 2018, thousands of apps have been investigated and around 200 apps have been suspended—pending a thorough investigation into whether they did in fact misuse any data. Where we find evidence that these or other apps did misuse data, we will ban them and let people know.

Facebook is generally not opposed to regulation but wants to ensure it is the right regulation. The issues facing the industry are complex, multi-faceted, and affect an important part of peoples' lives. As such, Facebook is absolutely committed to working with regulators, like Congress, to craft the right regulations. Facebook would be happy to review any proposed legislation and provide comments.

124. How long are third parties legally allowed to retain the user data that they got from Facebook (e.g. 1 yr, 5 yrs, forever)?

Facebook's policies regarding third-party usage of its platform technologies have prohibited—and continue to prohibit—third-party app developers from selling or licensing user data obtained from Facebook and from sharing any user data obtained from Facebook with any ad network, data broker or other advertising or monetization-related service.

We use a variety of tools to enforce Facebook policies against violating parties, including developers. We review tens of thousands of apps per year and regularly disapprove noncompliant apps as part of our proactive review process. We also use tools like cease and desist letters, account suspensions, letter agreements, and civil litigation. For example, since 2006, Facebook has sent over 1,150 cease-and-desist letters to over 1,600 targets. In 2017, we took action against about 370,000 apps, ranging from imposing certain restrictions to removal of the app from the platform. Moreover, we have required parties who have procured our data without authorization to delete that data. We have invested significant resources in these efforts.

Recently, we announced a number of additional steps we're taking to address concerns raised by Kogan's app.

- **Review our platform.** We will investigate all apps that had access to large amounts of data before the platform changes we announced in 2014, and we will audit any app where we identify suspicious activity. If we identify misuses of data, we'll take immediate action, including banning the app from our platform and pursuing legal action if appropriate.

- **Tell people about data misuse.** We will tell people about apps that have misused their data. This includes building a way for people to know if their data might have been accessed via the app. Moving forward, if we remove an app, we will tell people.

- **Turn off access for unused apps.** If someone has not used an app within the last three months, we will turn off the app's access to their data.

- **Restrict Facebook Login data.** We are changing Login, so that the only data that an app can request without app review will include name, profile photo, and email address. Requesting any other data will require approval from Facebook. We will also no longer allow apps to ask for access to information like religious or political views, relationship status and details, custom friends lists, education and work history, fitness activity, book reading and music listening activity, news reading, video watch activity, and games activity. We will encourage people to manage the apps they use. We already show people what apps their accounts are connected to and allow them to control what data they've permitted those apps to use. But we're making it easier for people to see what apps they use and the information they have shared with those apps.

- **Reward people who find vulnerabilities.** We launched the Data Abuse Bounty program so that people can report to us any misuses of data by app developers.

- **Update our policies.** We have updated our terms and Data Policy to explain how we use data and how data is shared with app developers.

125. Will you pledge to require all advertisers to disclose in detail their funding sources through methods including, but not limited to, notices attached to every single advertisement that appears on your site, which viewers can easily access by clicking a single link?

a. You recently stated that Facebook will support Sen. Klobuchar's Honest Ads Act. What other recommendations does Facebook have to improve regulation of political and other content on its sites? How will you go beyond the letter of the law of the Honest Ads Act?

b. Do you pledge that Facebook will work aggressively, proactively, and sincerely to ensure that your platform will be a positive contributor to the democratic process from now on, rather than an obstacle to fair and free elections as it was in 2016?

c. Will Facebook continue to use sophisticated methods to limit its federal taxes, or do you intend to take a more civic-minded approach to your business?

To build a secure product with extensive infrastructure that connects people wherever they live or whatever their income level, we need to make sure everyone can afford it. Advertising lets us keep Facebook free, which ensures it remains affordable for everyone. We also believe the ads you see across the Facebook family of apps and services should be useful

and relevant to you. Users can't opt out of seeing ads altogether because selling ads is what keeps Facebook free, but they do have different options to control how their data can and can't be used to show them ads. They're all found in ad preferences, which allows users to turn off the use of all data collected from partners off Facebook to target ads. Users can also decide which of their profile fields they want used for ad targeting in the Information section under "About you." Users can remove themselves from interests under "Your interests" and categories under "Your categories." And, we do not sell people's information to anyone, and we never will.

Facebook is committed to transparency for all ads, including ads with political content. Facebook believes that people should be able to easily understand why they are seeing ads, who paid for them, and what other ads those advertisers are running. As such, Facebook only allows authorized advertisers to run ads about elections or issues that are being debated across the country. In order to be authorized by Facebook, advertisers will need to confirm their identity and location. Furthermore, all political and issue ads will include a disclosure which reads: "Paid for by," and when users click on this disclosure they will be able to see details about the advertiser. Users will also be able to see an explanation of why they saw the particular ad. This is similar to the disclosure included on political TV advertisements. We just launched globally View Active Ads, a feature that will enable anyone to see all of the ads an advertiser is currently running by visiting the advertiser's Facebook Page.

126. Should the US recognize a web user's right to personal data privacy such as the EU has?

As a part of our overall approach to privacy, we are providing the same tools for access, rectification, erasure, data portability and others to people in the US (and globally) that we provide in the European Union under the GDPR. The controls and settings that Facebook is enabling as part of GDPR include settings for controlling our use of face recognition on Facebook and for controlling our ability to use data we collect off Facebook Company Products to target ads. We recently began providing direct notice of these controls and our updated terms to people around the world (including in the US), allowing people to choose whether or not to enable or disable these settings or to consent to our updated terms. Many of these tools (like our Download Your Information tool, ad preferences tool, and Activity Log) have been available globally for many years.

However, the GDPR creates some specific requirements that do not apply in the rest of the world, for example the requirement to provide contact information for the EU Data Protection Officer or to specify legal bases for processing data. We are also looking to be more responsive to regional norms and legal frameworks going forward, and want to have the flexibility to work with local regulators, which is possible with this new model. At the same time, we are changing the provisions in our Facebook, Inc. terms in our user agreements outside the United States to allow people in other countries to file lawsuits against Facebook in their home country, rather than in courts in the US. This transition was part of a continued effort to be locally responsive in countries where people use our services.

127. Can Facebook offer a fully private ad-free annual membership plan like an unlisted phone number?

To build a secure product with extensive infrastructure that connects people wherever they live or whatever their income level, we need to make sure everyone can afford it. Advertising lets us keep Facebook free, which ensures it remains affordable for everyone. We also believe the ads you see across the Facebook family of apps and services should be useful and relevant to you. Users can't opt out of seeing ads altogether because selling ads is what keeps Facebook free, but they do have different options to control how their data can and can't be used to show them ads. They're all found in ad preferences, which allows users to turn off the use of all data collected from partners off Facebook to target ads. Users can also decide which of their profile fields they want used for ad targeting in the Information section under "About you." Users can remove themselves from interests under "Your interests" and categories under "Your categories." And, we do not sell people's information to anyone, and we never will.

Facebook is committed to transparency for all ads, including ads with political content. Facebook believes that people should be able to easily understand why they are seeing ads, who paid for them, and what other ads those advertisers are running. As such, Facebook only allows authorized advertisers to run ads about elections or issues that are being debated across the country. In order to be authorized by Facebook, advertisers will need to confirm their identity and location. Furthermore, all political and issue ads will include a disclosure which reads: "Paid for by," and when users click on this disclosure they will be able to see details about the advertiser. Users will also be able to see an explanation of why they saw the particular ad. This is similar to the disclosure included on political TV advertisements. We just launched globally View Active Ads, a feature that will enable anyone to see all of the ads an advertiser is currently running by visiting the advertiser's Facebook Page.

128. Mr. Zuckerberg, Facebook is already operating in European countries with much stricter privacy laws. What is stopping you from applying your already existing stricter European software to your American customers? We understand that if you sell less personal data you will make less income. At what point do you demand decency over dollars?

As a part of our overall approach to privacy, we are providing the same tools for access, rectification, erasure, data portability and others to people in the US (and globally) that we provide in the European Union under the GDPR. The controls and settings that Facebook is enabling as part of GDPR include settings for controlling our use of face recognition on Facebook and for controlling our ability to use data we collect off Facebook Company Products to target ads. We recently began providing direct notice of these controls and our updated terms to people around the world (including in the US), allowing people to choose whether or not to enable or disable these settings or to consent to our updated terms. Many of these tools (like our Download Your Information tool, ad preferences tool, and Activity Log) have been available globally for many years.

However, the GDPR creates some specific requirements that do not apply in the rest of the world, for example the requirement to provide contact information for the EU Data Protection Officer or to specify legal bases for processing data. We are also looking to be more responsive to regional norms and legal frameworks going forward, and want to have the flexibility to work with local regulators, which is possible with this new model. At the same time, we are changing the provisions in our Facebook, Inc. terms in our user agreements outside

the United States to allow people in other countries to file lawsuits against Facebook in their home country, rather than in courts in the US. This transition was part of a continued effort to be locally responsive in countries where people use our services.

129. How will you protect user's privacy?

We believe everyone deserves good privacy controls. A user owns the information they share on Facebook. This means they decide what they share and who they share it with on Facebook, and they can change their mind. We require websites and apps who use our tools to tell users they're collecting and sharing their information with us, and to get users' permission to do so.

Everyone has the right to expect strong protections for their information. We also need to do our part to help keep our community safe, in a way that's consistent with people's privacy expectations. We've recently announced several steps to give people more control over their privacy, including a new Privacy Shortcuts tool that we're rolling out now to give people information about how to control their information, including choosing who can see what they post and adding protections like two-factor authentication to their account. People can learn more about how to protect their privacy in our updated Data Policy and in our Privacy Basics feature (https://www.facebook.com/about/basics).

We are in the process of investigating every app that had access to a large amount of information before we changed our Platform in 2014. The investigation process is in full swing. We have large teams of internal and external experts working hard to investigate these apps as quickly as possible. As of early June 2018, thousands of apps have been investigated and around 200 apps have been suspended—pending a thorough investigation into whether they did in fact misuse any data. Where we find evidence that these or other apps did misuse data, we will ban them and let people know.

Facebook is generally not opposed to regulation but wants to ensure it is the right regulation. The issues facing the industry are complex, multi-faceted, and affect an important part of peoples' lives. As such, Facebook is absolutely committed to working with regulators, like Congress, to craft the right regulations. Facebook would be happy to review any proposed legislation and provide comments.

130. What do you think Facebook's responsibility is to protect data & privacy of your users?

We believe everyone deserves good privacy controls. A user owns the information they share on Facebook. This means they decide what they share and who they share it with on Facebook, and they can change their mind. We require websites and apps who use our tools to tell users they're collecting and sharing their information with us, and to get users' permission to do so.

Everyone has the right to expect strong protections for their information. We also need to do our part to help keep our community safe, in a way that's consistent with people's privacy expectations. We've recently announced several steps to give people more control over their privacy, including a new Privacy Shortcuts tool that we're rolling out now to give people

information about how to control their information, including choosing who can see what they post and adding protections like two-factor authentication to their account. People can learn more about how to protect their privacy in our updated Data Policy and in our Privacy Basics feature (https://www.facebook.com/about/basics).

We are in the process of investigating every app that had access to a large amount of information before we changed our Platform in 2014. The investigation process is in full swing. We have large teams of internal and external experts working hard to investigate these apps as quickly as possible. As of early June 2018, thousands of apps have been investigated and around 200 apps have been suspended—pending a thorough investigation into whether they did in fact misuse any data. Where we find evidence that these or other apps did misuse data, we will ban them and let people know.

Facebook is generally not opposed to regulation but wants to ensure it is the right regulation. The issues facing the industry are complex, multi-faceted, and affect an important part of peoples' lives. As such, Facebook is absolutely committed to working with regulators, like Congress, to craft the right regulations. Facebook would be happy to review any proposed legislation and provide comments.

131. When can you implement plagiarism-detection software to ID & intercept propaganda?

We want Facebook to be a place where people can discover more news, information, and perspectives, and we are working to build products that help to that. Through our News Feed algorithm, we also work hard to actively reduce the distribution of clickbait, sensationalism, and misinformation, on the one hand, and to boost news and information from sources that are trusted, informative, and local, on the other hand.

We are focusing on four different strategies to address misinformation:

- **Strengthening enforcement of our authenticity policies.** We are investing heavily in new technology and hiring thousands more people to tackle the problem of inauthenticity on the platform. Fake accounts are often associated with false news, so this is an area that will have a huge impact on curbing the spread of inaccurate information.

- **Finding industry solutions.** All of us—from tech companies and media companies to newsrooms and classrooms—must work together to find industry solutions to strengthen the online news ecosystem and our own digital literacy. That's why we're collaborating with others who operate in this space. Last January, we announced The Facebook Journalism Project, an initiative that seeks to establish stronger ties between Facebook and the news industry. The project is focused on developing news products, providing training and tools for journalists, and working with publishers and educators on how we can equip people with the knowledge they need to be informed readers in the digital age. Since launching the Journalism Project, we've met with more than 2,600 publishers around the world to understand how they use our products and how we can make improvements to better support their needs.

- **Disrupting economic incentives.** When it comes to fighting false news, we've found that a lot of it is financially motivated. So, one of the most effective approaches is removing the economic incentives for those who traffic in inaccurate information. We've done things like block ads from pages that repeatedly share false news and significantly limit the distribution of web pages that deliver low quality web experiences.

- **Building new products.** We believe it's important to amplify the good effects of social media and mitigate the bad—to contribute to the diversity of ideas, information, and view points, while strengthening our common understanding.

    - We believe giving people more context can help them decide what to trust and what to share. The third-party fact-checking program we have developed uses reports from our community, along with other signals, to send stories to accredited third-party fact checking organizations. If the fact checking organizations identify a story as fake, we will suggest related articles in News Feed to show people different points of view, including information from fact checkers. Stories that have been disputed may also appear lower in News Feed. Our own data analytics show that a false rating from one of our fact checking partners reduces future impressions on Facebook by 80 percent.

    - We're also testing Article Context as a way of giving people more information about the material they're reading on Facebook. Since we launched this test, some of the articles people see in News Feed will feature an "i" icon that allows them to access more information at the tap of a button. The information we surface is pulled from across the internet, and includes things like the publisher's Wikipedia entry, trending articles or related articles about the topic, and information about how the article is being shared on Facebook. In some cases, if that information is unavailable, we will let people know since that can also be helpful context.

132. Haven't you monetized people's need to be connected with family and friends? You say it's free but the cost Facebook users pay is to lose their personal information about themselves and their relationships with others to people who just want them to fear more and spend more. Isn't Facebook just a form of data mining?

We believe that it's important to communicate with people about the information that we collect and how people can control it. As explained in our Data Policy, we collect three basic categories of data about people:

(1) data about things people do and share (and who they connect with) on our services;

(2) data about the devices people use to access our services; and

(3) data we receive from partners, including the websites and apps that use our business tools.

We collect information about the people, Pages, accounts, hashtags, and groups users are connected to and how they interact with them across our Products, such as people a user communicates with the most or groups users are part of. We also collect contact information if they choose to upload, sync, or import it from a device (such as an address book or call log or SMS log history), which we use for things like helping them and others find people they may know.

The data we use to show ads to people depends on the data we have received from people. For people who are new to Facebook, we may have minimal data that we can use. For people who have used our services for longer, we likely have more data, but the amount of data will depend on the nature of that use and how they have used our controls. Any person can see each of the specific interests we maintain about them for advertising by visiting Ads Preferences, which lets people see what interests we use to choose ads for them—and to edit or delete these interests. We also provide more detailed information about how we use data to decide what ads to show to people in our "About Facebook Ads" page, at https://www.facebook.com/ads/about. And, we do not sell people's information to anyone, and we never will.

All users must expressly consent to Facebook's Terms and Data Policy when registering for Facebook. The Data Policy explains the kinds of information we collect, how we use this information, how we share this information, and how users can manage and delete information.

Facebook does not create profiles for people without a Facebook account, but we do receive some information from devices and browsers that may be used by non-users. For example:

- When people visit apps or websites that feature our technologies—like the Facebook Like or Comment button—our servers automatically log (i) standard browser or app records of the fact that a particular device or user visited the website or app (this connection to Facebook's servers occurs automatically when a person visits a website or app that contains our technologies, such as a Like button, and is an inherent function of Internet design); and (ii) any additional information the publisher of the app or website chooses to share with Facebook about the person's activities on that site (such as the fact that a purchase was made on the site). This is a standard feature of the Internet, and most websites and apps share this same information with multiple different third-parties whenever people visit their website or app. When the person visiting a website featuring Facebook's tools is not a registered Facebook user, Facebook does not have information identifying that individual, and it does not create profiles for this individual.

- We also may receive information about the device of a non-registered user if that user visits a part of Facebook that does not require people to log in—such as a public Facebook Page. The information we log when people visit our websites or apps is the same as described above and is the same information that any provider of an online service would receive.

- In addition, Facebook may receive some basic information about devices where Facebook apps are installed, including before people using those devices have registered for Facebook (such as when a user downloads a Facebook app, but has not yet created an

account, or if the app is preloaded on a given device). This device data includes things like device model, operating system, IP address, app version and device identifiers. We use this information to provide the right version of the app, help people who want to create accounts (for example, optimizing the registration flow for the specific device), retrieving bug fixes and measuring and improving app performance. We do not use this information to build profiles about non-registered users.

133. Why should we trust you again with our important information, our friend's contacts and our family secrets? Information that could be used against us, and was used against our Democratic elections process. Information that could be sold on the black market steal our identities.

We believe everyone deserves good privacy controls. A user owns the information they share on Facebook. This means they decide what they share and who they share it with on Facebook, and they can change their mind. We require websites and apps who use our tools to tell users they're collecting and sharing their information with us, and to get users' permission to do so.

Everyone has the right to expect strong protections for their information. We also need to do our part to help keep our community safe, in a way that's consistent with people's privacy expectations. We've recently announced several steps to give people more control over their privacy, including a new Privacy Shortcuts tool that we're rolling out now to give people information about how to control their information, including choosing who can see what they post and adding protections like two-factor authentication to their account. People can learn more about how to protect their privacy in our updated Data Policy and in our Privacy Basics feature (https://www.facebook.com/about/basics).

We are in the process of investigating every app that had access to a large amount of information before we changed our Platform in 2014. The investigation process is in full swing. We have large teams of internal and external experts working hard to investigate these apps as quickly as possible. As of early June 2018, thousands of apps have been investigated and around 200 apps have been suspended—pending a thorough investigation into whether they did in fact misuse any data. Where we find evidence that these or other apps did misuse data, we will ban them and let people know.

Facebook is generally not opposed to regulation but wants to ensure it is the right regulation. The issues facing the industry are complex, multi-faceted, and affect an important part of peoples' lives. As such, Facebook is absolutely committed to working with regulators, like Congress, to craft the right regulations. Facebook would be happy to review any proposed legislation and provide comments.

134. What is his plan to prevent such data breaches in the future to keep users safe?

Facebook's policies regarding third-party usage of its platform technologies have prohibited—and continue to prohibit—third-party app developers from selling or licensing user data obtained from Facebook and from sharing any user data obtained from Facebook with any ad network, data broker or other advertising or monetization-related service.

We use a variety of tools to enforce Facebook policies against violating parties, including developers. We review tens of thousands of apps per year and regularly disapprove noncompliant apps as part of our proactive review process. We also use tools like cease and desist letters, account suspensions, letter agreements, and civil litigation. For example, since 2006, Facebook has sent over 1,150 cease-and-desist letters to over 1,600 targets. In 2017, we took action against about 370,000 apps, ranging from imposing certain restrictions to removal of the app from the platform. Moreover, we have required parties who have procured our data without authorization to delete that data. We have invested significant resources in these efforts.

Recently, we announced a number of additional steps we're taking to address concerns raised by Kogan's app.

- **Review our platform.** We will investigate all apps that had access to large amounts of data before the platform changes we announced in 2014, and we will audit any app where we identify suspicious activity. If we identify misuses of data, we'll take immediate action, including banning the app from our platform and pursuing legal action if appropriate.

- **Tell people about data misuse.** We will tell people about apps that have misused their data. This includes building a way for people to know if their data might have been accessed via the app. Moving forward, if we remove an app, we will tell people.

- **Turn off access for unused apps.** If someone has not used an app within the last three months, we will turn off the app's access to their data.

- **Restrict Facebook Login data.** We are changing Login, so that the only data that an app can request without app review will include name, profile photo, and email address. Requesting any other data will require approval from Facebook. We will also no longer allow apps to ask for access to information like religious or political views, relationship status and details, custom friends lists, education and work history, fitness activity, book reading and music listening activity, news reading, video watch activity, and games activity. We will encourage people to manage the apps they use. We already show people what apps their accounts are connected to and allow them to control what data they've permitted those apps to use. But we're making it easier for people to see what apps they use and the information they have shared with those apps.

- **Reward people who find vulnerabilities.** We launched the Data Abuse Bounty program so that people can report to us any misuses of data by app developers.

- **Update our policies.** We have updated our terms and Data Policy to explain how we use data and how data is shared with app developers.

135. Can we get the names of ALL individuals and organizations that Facebook has shared users' private data with and when was it shared?

Facebook's policies regarding third-party usage of its platform technologies have prohibited—and continue to prohibit—third-party app developers from selling or licensing user data obtained from Facebook and from sharing any user data obtained from Facebook with any ad network, data broker or other advertising or monetization-related service.

We use a variety of tools to enforce Facebook policies against violating parties, including developers. We review tens of thousands of apps per year and regularly disapprove noncompliant apps as part of our proactive review process. We also use tools like cease and desist letters, account suspensions, letter agreements, and civil litigation. For example, since 2006, Facebook has sent over 1,150 cease-and-desist letters to over 1,600 targets. In 2017, we took action against about 370,000 apps, ranging from imposing certain restrictions to removal of the app from the platform. Moreover, we have required parties who have procured our data without authorization to delete that data. We have invested significant resources in these efforts.

Recently, we announced a number of additional steps we're taking to address concerns raised by Kogan's app.

- Review our platform. We will investigate all apps that had access to large amounts of data before the platform changes we announced in 2014, and we will audit any app where we identify suspicious activity. If we identify misuses of data, we'll take immediate action, including banning the app from our platform and pursuing legal action if appropriate.

- Tell people about data misuse. We will tell people about apps that have misused their data. This includes building a way for people to know if their data might have been accessed via the app. Moving forward, if we remove an app, we will tell people.

- Turn off access for unused apps. If someone has not used an app within the last three months, we will turn off the app's access to their data.

- Restrict Facebook Login data. We are changing Login, so that the only data that an app can request without app review will include name, profile photo, and email address. Requesting any other data will require approval from Facebook. We will also no longer allow apps to ask for access to information like religious or political views, relationship status and details, custom friends lists, education and work history, fitness activity, book reading and music listening activity, news reading, video watch activity, and games activity. We will encourage people to manage the apps they use. We already show people what apps their accounts are connected to and allow them to control what data they've permitted those apps to use. But we're making it easier for people to see what apps they use and the information they have shared with those apps.

- Reward people who find vulnerabilities. We launched the Data Abuse Bounty program so that people can report to us any misuses of data by app developers.

- Update our policies. We have updated our terms and Data Policy to explain how we use data and how data is shared with app developers.

136. Ask him why he and his company reneged on his promise to the BBC back in 2009 that the person who owns the data is the one who put it there.

We believe that it's important to communicate with people about the information that we collect and how people can control it. As explained in our Data Policy, we collect three basic categories of data about people:

(1) data about things people do and share (and who they connect with) on our services;

(2) data about the devices people use to access our services; and

(3) data we receive from partners, including the websites and apps that use our business tools.

We collect information about the people, Pages, accounts, hashtags, and groups users are connected to and how they interact with them across our Products, such as people a user communicates with the most or groups users are part of. We also collect contact information if they choose to upload, sync, or import it from a device (such as an address book or call log or SMS log history), which we use for things like helping them and others find people they may know.

The data we use to show ads to people depends on the data we have received from people. For people who are new to Facebook, we may have minimal data that we can use. For people who have used our services for longer, we likely have more data, but the amount of data will depend on the nature of that use and how they have used our controls. Any person can see each of the specific interests we maintain about them for advertising by visiting Ads Preferences, which lets people see what interests we use to choose ads for them—and to edit or delete these interests. We also provide more detailed information about how we use data to decide what ads to show to people in our "About Facebook Ads" page, at https://www.facebook.com/ads/about. And, we do not sell people's information to anyone, and we never will.

All users must expressly consent to Facebook's Terms and Data Policy when registering for Facebook. The Data Policy explains the kinds of information we collect, how we use this information, how we share this information, and how users can manage and delete information.

Facebook does not create profiles for people without a Facebook account, but we do receive some information from devices and browsers that may be used by non-users. For example:

- When people visit apps or websites that feature our technologies—like the Facebook Like or Comment button—our servers automatically log (i) standard browser or app records of the fact that a particular device or user visited the website or app (this connection to Facebook's servers occurs automatically when a person visits a website or app that contains our technologies, such as a Like button, and is an inherent function of Internet design); and (ii) any additional information the publisher of the app or website chooses to share with Facebook about the person's activities on that site (such as the fact that a purchase was made on the site). This is a standard feature of the Internet, and most websites and apps share this same information with multiple different third-parties

whenever people visit their website or app. When the person visiting a website featuring Facebook's tools is not a registered Facebook user, Facebook does not have information identifying that individual, and it does not create profiles for this individual.

- We also may receive information about the device of a non-registered user if that user visits a part of Facebook that does not require people to log in—such as a public Facebook Page. The information we log when people visit our websites or apps is the same as described above and is the same information that any provider of an online service would receive.

- In addition, Facebook may receive some basic information about devices where Facebook apps are installed, including before people using those devices have registered for Facebook (such as when a user downloads a Facebook app, but has not yet created an account, or if the app is preloaded on a given device). This device data includes things like device model, operating system, IP address, app version and device identifiers. We use this information to provide the right version of the app, help people who want to create accounts (for example, optimizing the registration flow for the specific device), retrieving bug fixes and measuring and improving app performance. We do not use this information to build profiles about non-registered users.

137. Why doesn't Facebook make the default setting MAXIMUM PRIVACY?

We believe everyone deserves good privacy controls. A user owns the information they share on Facebook. This means they decide what they share and who they share it with on Facebook, and they can change their mind. We require websites and apps who use our tools to tell users they're collecting and sharing their information with us, and to get users' permission to do so.

Everyone has the right to expect strong protections for their information. We also need to do our part to help keep our community safe, in a way that's consistent with people's privacy expectations. We've recently announced several steps to give people more control over their privacy, including a new Privacy Shortcuts tool that we're rolling out now to give people information about how to control their information, including choosing who can see what they post and adding protections like two-factor authentication to their account. People can learn more about how to protect their privacy in our updated Data Policy and in our Privacy Basics feature (https://www.facebook.com/about/basics).

We are in the process of investigating every app that had access to a large amount of information before we changed our Platform in 2014. The investigation process is in full swing. We have large teams of internal and external experts working hard to investigate these apps as quickly as possible. As of early June 2018, thousands of apps have been investigated and around 200 apps have been suspended—pending a thorough investigation into whether they did in fact misuse any data. Where we find evidence that these or other apps did misuse data, we will ban them and let people know.

Facebook is generally not opposed to regulation but wants to ensure it is the right regulation. The issues facing the industry are complex, multi-faceted, and affect an important

part of peoples' lives. As such, Facebook is absolutely committed to working with regulators, like Congress, to craft the right regulations. Facebook would be happy to review any proposed legislation and provide comments.

138. How much would the service cost for consumers to maintain their privacy? Would Facebook still be as popular?

We believe everyone deserves good privacy controls. A user owns the information they share on Facebook. This means they decide what they share and who they share it with on Facebook, and they can change their mind. We require websites and apps who use our tools to tell users they're collecting and sharing their information with us, and to get users' permission to do so.

Everyone has the right to expect strong protections for their information. We also need to do our part to help keep our community safe, in a way that's consistent with people's privacy expectations. We've recently announced several steps to give people more control over their privacy, including a new Privacy Shortcuts tool that we're rolling out now to give people information about how to control their information, including choosing who can see what they post and adding protections like two-factor authentication to their account. People can learn more about how to protect their privacy in our updated Data Policy and in our Privacy Basics feature (https://www.facebook.com/about/basics).

We are in the process of investigating every app that had access to a large amount of information before we changed our Platform in 2014. The investigation process is in full swing. We have large teams of internal and external experts working hard to investigate these apps as quickly as possible. As of early June 2018, thousands of apps have been investigated and around 200 apps have been suspended—pending a thorough investigation into whether they did in fact misuse any data. Where we find evidence that these or other apps did misuse data, we will ban them and let people know.

Facebook is generally not opposed to regulation but wants to ensure it is the right regulation. The issues facing the industry are complex, multi-faceted, and affect an important part of peoples' lives. As such, Facebook is absolutely committed to working with regulators, like Congress, to craft the right regulations. Facebook would be happy to review any proposed legislation and provide comments.

139. You've already broken your past privacy promise. How can we trust you to protect our privacy now?

We believe everyone deserves good privacy controls. A user owns the information they share on Facebook. This means they decide what they share and who they share it with on Facebook, and they can change their mind. We require websites and apps who use our tools to tell users they're collecting and sharing their information with us, and to get users' permission to do so.

Everyone has the right to expect strong protections for their information. We also need to do our part to help keep our community safe, in a way that's consistent with people's privacy expectations. We've recently announced several steps to give people more control over their privacy, including a new Privacy Shortcuts tool that we're rolling out now to give people information about how to control their information, including choosing who can see what they post and adding protections like two-factor authentication to their account. People can learn more about how to protect their privacy in our updated Data Policy and in our Privacy Basics feature (https://www.facebook.com/about/basics).

We are in the process of investigating every app that had access to a large amount of information before we changed our Platform in 2014. The investigation process is in full swing. We have large teams of internal and external experts working hard to investigate these apps as quickly as possible. As of early June 2018, thousands of apps have been investigated and around 200 apps have been suspended—pending a thorough investigation into whether they did in fact misuse any data. Where we find evidence that these or other apps did misuse data, we will ban them and let people know.

Facebook is generally not opposed to regulation but wants to ensure it is the right regulation. The issues facing the industry are complex, multi-faceted, and affect an important part of peoples' lives. As such, Facebook is absolutely committed to working with regulators, like Congress, to craft the right regulations. Facebook would be happy to review any proposed legislation and provide comments.

140. How do you plan to protect individuals' privacy and data from use by others without specific written?

We believe everyone deserves good privacy controls. A user owns the information they share on Facebook. This means they decide what they share and who they share it with on Facebook, and they can change their mind. We require websites and apps who use our tools to tell users they're collecting and sharing their information with us, and to get users' permission to do so.

Everyone has the right to expect strong protections for their information. We also need to do our part to help keep our community safe, in a way that's consistent with people's privacy expectations. We've recently announced several steps to give people more control over their privacy, including a new Privacy Shortcuts tool that we're rolling out now to give people information about how to control their information, including choosing who can see what they post and adding protections like two-factor authentication to their account. People can learn more about how to protect their privacy in our updated Data Policy and in our Privacy Basics feature (https://www.facebook.com/about/basics).

We are in the process of investigating every app that had access to a large amount of information before we changed our Platform in 2014. The investigation process is in full swing. We have large teams of internal and external experts working hard to investigate these apps as quickly as possible. As of early June 2018, thousands of apps have been investigated and around 200 apps have been suspended—pending a thorough investigation into whether they did in fact

misuse any data. Where we find evidence that these or other apps did misuse data, we will ban them and let people know.

Facebook is generally not opposed to regulation but wants to ensure it is the right regulation. The issues facing the industry are complex, multi-faceted, and affect an important part of peoples' lives. As such, Facebook is absolutely committed to working with regulators, like Congress, to craft the right regulations. Facebook would be happy to review any proposed legislation and provide comments.

141. When are you going to seriously protect user data and stop exploiting it?

We believe everyone deserves good privacy controls. A user owns the information they share on Facebook. This means they decide what they share and who they share it with on Facebook, and they can change their mind. We require websites and apps who use our tools to tell users they're collecting and sharing their information with us, and to get users' permission to do so.

Everyone has the right to expect strong protections for their information. We also need to do our part to help keep our community safe, in a way that's consistent with people's privacy expectations. We've recently announced several steps to give people more control over their privacy, including a new Privacy Shortcuts tool that we're rolling out now to give people information about how to control their information, including choosing who can see what they post and adding protections like two-factor authentication to their account. People can learn more about how to protect their privacy in our updated Data Policy and in our Privacy Basics feature (https://www.facebook.com/about/basics).

We are in the process of investigating every app that had access to a large amount of information before we changed our Platform in 2014. The investigation process is in full swing. We have large teams of internal and external experts working hard to investigate these apps as quickly as possible. As of early June 2018, thousands of apps have been investigated and around 200 apps have been suspended—pending a thorough investigation into whether they did in fact misuse any data. Where we find evidence that these or other apps did misuse data, we will ban them and let people know.

Facebook is generally not opposed to regulation but wants to ensure it is the right regulation. The issues facing the industry are complex, multi-faceted, and affect an important part of peoples' lives. As such, Facebook is absolutely committed to working with regulators, like Congress, to craft the right regulations. Facebook would be happy to review any proposed legislation and provide comments.

142. Why isn't "Opt Out" the default for everything? Why not only as for 'Opt In' when someone accesses a feature that might need it?

We believe everyone deserves good privacy controls. A user owns the information they share on Facebook. This means they decide what they share and who they share it with on Facebook, and they can change their mind. We require websites and apps who use our tools to tell users they're collecting and sharing their information with us, and to get users' permission to do so.

Everyone has the right to expect strong protections for their information. We also need to do our part to help keep our community safe, in a way that's consistent with people's privacy expectations. We've recently announced several steps to give people more control over their privacy, including a new Privacy Shortcuts tool that we're rolling out now to give people information about how to control their information, including choosing who can see what they post and adding protections like two-factor authentication to their account. People can learn more about how to protect their privacy in our updated Data Policy and in our Privacy Basics feature (https://www.facebook.com/about/basics).

We are in the process of investigating every app that had access to a large amount of information before we changed our Platform in 2014. The investigation process is in full swing. We have large teams of internal and external experts working hard to investigate these apps as quickly as possible. As of early June 2018, thousands of apps have been investigated and around 200 apps have been suspended—pending a thorough investigation into whether they did in fact misuse any data. Where we find evidence that these or other apps did misuse data, we will ban them and let people know.

Facebook is generally not opposed to regulation but wants to ensure it is the right regulation. The issues facing the industry are complex, multi-faceted, and affect an important part of peoples' lives. As such, Facebook is absolutely committed to working with regulators, like Congress, to craft the right regulations. Facebook would be happy to review any proposed legislation and provide comments.

143. Why are you willing to risk our democracy by selling your customers privacy merely to make money?

We believe everyone deserves good privacy controls. A user owns the information they share on Facebook. This means they decide what they share and who they share it with on Facebook, and they can change their mind. We require websites and apps who use our tools to tell users they're collecting and sharing their information with us, and to get users' permission to do so.

Everyone has the right to expect strong protections for their information. We also need to do our part to help keep our community safe, in a way that's consistent with people's privacy expectations. We've recently announced several steps to give people more control over their privacy, including a new Privacy Shortcuts tool that we're rolling out now to give people information about how to control their information, including choosing who can see what they post and adding protections like two-factor authentication to their account. People can learn more about how to protect their privacy in our updated Data Policy and in our Privacy Basics feature (https://www.facebook.com/about/basics).

We are in the process of investigating every app that had access to a large amount of information before we changed our Platform in 2014. The investigation process is in full swing. We have large teams of internal and external experts working hard to investigate these apps as quickly as possible. As of early June 2018, thousands of apps have been investigated and around 200 apps have been suspended—pending a thorough investigation into whether they did in fact

misuse any data. Where we find evidence that these or other apps did misuse data, we will ban them and let people know.

Facebook is generally not opposed to regulation but wants to ensure it is the right regulation. The issues facing the industry are complex, multi-faceted, and affect an important part of peoples' lives. As such, Facebook is absolutely committed to working with regulators, like Congress, to craft the right regulations. Facebook would be happy to review any proposed legislation and provide comments.

144. Is it possible to 100% protect user data?

We believe everyone deserves good privacy controls. A user owns the information they share on Facebook. This means they decide what they share and who they share it with on Facebook, and they can change their mind. We require websites and apps who use our tools to tell users they're collecting and sharing their information with us, and to get users' permission to do so.

Everyone has the right to expect strong protections for their information. We also need to do our part to help keep our community safe, in a way that's consistent with people's privacy expectations. We've recently announced several steps to give people more control over their privacy, including a new Privacy Shortcuts tool that we're rolling out now to give people information about how to control their information, including choosing who can see what they post and adding protections like two-factor authentication to their account. People can learn more about how to protect their privacy in our updated Data Policy and in our Privacy Basics feature (https://www.facebook.com/about/basics).

We are in the process of investigating every app that had access to a large amount of information before we changed our Platform in 2014. The investigation process is in full swing. We have large teams of internal and external experts working hard to investigate these apps as quickly as possible. As of early June 2018, thousands of apps have been investigated and around 200 apps have been suspended—pending a thorough investigation into whether they did in fact misuse any data. Where we find evidence that these or other apps did misuse data, we will ban them and let people know.

Facebook is generally not opposed to regulation but wants to ensure it is the right regulation. The issues facing the industry are complex, multi-faceted, and affect an important part of peoples' lives. As such, Facebook is absolutely committed to working with regulators, like Congress, to craft the right regulations. Facebook would be happy to review any proposed legislation and provide comments.

145. What steps to limit access to users' data had Facebook considered but implemented prior to these breaches? For what reasons, apart from technical limitations, were they not implemented?

We believe that it's important to communicate with people about the information that we collect and how people can control it. As explained in our Data Policy, we collect three basic categories of data about people:

(1) data about things people do and share (and who they connect with) on our services;

(2) data about the devices people use to access our services; and

(3) data we receive from partners, including the websites and apps that use our business tools.

We collect information about the people, Pages, accounts, hashtags, and groups users are connected to and how they interact with them across our Products, such as people a user communicates with the most or groups users are part of. We also collect contact information if they choose to upload, sync, or import it from a device (such as an address book or call log or SMS log history), which we use for things like helping them and others find people they may know.

The data we use to show ads to people depends on the data we have received from people. For people who are new to Facebook, we may have minimal data that we can use. For people who have used our services for longer, we likely have more data, but the amount of data will depend on the nature of that use and how they have used our controls. Any person can see each of the specific interests we maintain about them for advertising by visiting Ads Preferences, which lets people see what interests we use to choose ads for them—and to edit or delete these interests. We also provide more detailed information about how we use data to decide what ads to show to people in our "About Facebook Ads" page, at https://www.facebook.com/ads/about. And, we do not sell people's information to anyone, and we never will.

All users must expressly consent to Facebook's Terms and Data Policy when registering for Facebook. The Data Policy explains the kinds of information we collect, how we use this information, how we share this information, and how users can manage and delete information.

Facebook does not create profiles for people without a Facebook account, but we do receive some information from devices and browsers that may be used by non-users. For example:

- When people visit apps or websites that feature our technologies—like the Facebook Like or Comment button—our servers automatically log (i) standard browser or app records of the fact that a particular device or user visited the website or app (this connection to Facebook's servers occurs automatically when a person visits a website or app that contains our technologies, such as a Like button, and is an inherent function of Internet design); and (ii) any additional information the publisher of the app or website chooses to share with Facebook about the person's activities on that site (such as the fact that a purchase was made on the site). This is a standard feature of the Internet, and most websites and apps share this same information with multiple different third-parties whenever people visit their website or app. When the person visiting a website featuring Facebook's tools is not a registered Facebook user, Facebook does not have information identifying that individual, and it does not create profiles for this individual.

- We also may receive information about the device of a non-registered user if that user visits a part of Facebook that does not require people to log in—such as a public

Facebook Page. The information we log when people visit our websites or apps is the same as described above and is the same information that any provider of an online service would receive.

- In addition, Facebook may receive some basic information about devices where Facebook apps are installed, including before people using those devices have registered for Facebook (such as when a user downloads a Facebook app, but has not yet created an account, or if the app is preloaded on a given device). This device data includes things like device model, operating system, IP address, app version and device identifiers. We use this information to provide the right version of the app, help people who want to create accounts (for example, optimizing the registration flow for the specific device), retrieving bug fixes and measuring and improving app performance. We do not use this information to build profiles about non-registered users.

146. What distribution and publishing rights does Facebook have to user's info and uploaded files?

We believe that it's important to communicate with people about the information that we collect and how people can control it. As explained in our Data Policy, we collect three basic categories of data about people:

(1) data about things people do and share (and who they connect with) on our services;

(2) data about the devices people use to access our services; and

(3) data we receive from partners, including the websites and apps that use our business tools.

We collect information about the people, Pages, accounts, hashtags, and groups users are connected to and how they interact with them across our Products, such as people a user communicates with the most or groups users are part of. We also collect contact information if they choose to upload, sync, or import it from a device (such as an address book or call log or SMS log history), which we use for things like helping them and others find people they may know.

The data we use to show ads to people depends on the data we have received from people. For people who are new to Facebook, we may have minimal data that we can use. For people who have used our services for longer, we likely have more data, but the amount of data will depend on the nature of that use and how they have used our controls. Any person can see each of the specific interests we maintain about them for advertising by visiting Ads Preferences, which lets people see what interests we use to choose ads for them—and to edit or delete these interests. We also provide more detailed information about how we use data to decide what ads to show to people in our "About Facebook Ads" page, at https://www.facebook.com/ads/about. And, we do not sell people's information to anyone, and we never will.

All users must expressly consent to Facebook's Terms and Data Policy when registering for Facebook. The Data Policy explains the kinds of information we collect, how we use this information, how we share this information, and how users can manage and delete information.

Facebook does not create profiles for people without a Facebook account, but we do receive some information from devices and browsers that may be used by non-users. For example:

- When people visit apps or websites that feature our technologies—like the Facebook Like or Comment button—our servers automatically log (i) standard browser or app records of the fact that a particular device or user visited the website or app (this connection to Facebook's servers occurs automatically when a person visits a website or app that contains our technologies, such as a Like button, and is an inherent function of Internet design); and (ii) any additional information the publisher of the app or website chooses to share with Facebook about the person's activities on that site (such as the fact that a purchase was made on the site). This is a standard feature of the Internet, and most websites and apps share this same information with multiple different third-parties whenever people visit their website or app. When the person visiting a website featuring Facebook's tools is not a registered Facebook user, Facebook does not have information identifying that individual, and it does not create profiles for this individual.

- We also may receive information about the device of a non-registered user if that user visits a part of Facebook that does not require people to log in—such as a public Facebook Page. The information we log when people visit our websites or apps is the same as described above and is the same information that any provider of an online service would receive.

- In addition, Facebook may receive some basic information about devices where Facebook apps are installed, including before people using those devices have registered for Facebook (such as when a user downloads a Facebook app, but has not yet created an account, or if the app is preloaded on a given device). This device data includes things like device model, operating system, IP address, app version and device identifiers. We use this information to provide the right version of the app, help people who want to create accounts (for example, optimizing the registration flow for the specific device), retrieving bug fixes and measuring and improving app performance. We do not use this information to build profiles about non-registered users.

147. Why were they seeking patient records from hospitals? What is off limits for them? For Congress? For Citizens?

As discussed with your staff, this question is not germane to the hearing.

148. Describe in detail how you are now protecting the privacy of your subscribers.

We believe everyone deserves good privacy controls. A user owns the information they share on Facebook. This means they decide what they share and who they share it with on Facebook, and they can change their mind. We require websites and apps who use our tools to tell users they're collecting and sharing their information with us, and to get users' permission to do so.

Everyone has the right to expect strong protections for their information. We also need to do our part to help keep our community safe, in a way that's consistent with people's privacy expectations. We've recently announced several steps to give people more control over their privacy, including a new Privacy Shortcuts tool that we're rolling out now to give people information about how to control their information, including choosing who can see what they post and adding protections like two-factor authentication to their account. People can learn more about how to protect their privacy in our updated Data Policy and in our Privacy Basics feature (https://www.facebook.com/about/basics).

We are in the process of investigating every app that had access to a large amount of information before we changed our Platform in 2014. The investigation process is in full swing. We have large teams of internal and external experts working hard to investigate these apps as quickly as possible. As of early June 2018, thousands of apps have been investigated and around 200 apps have been suspended—pending a thorough investigation into whether they did in fact misuse any data. Where we find evidence that these or other apps did misuse data, we will ban them and let people know.

Facebook is generally not opposed to regulation but wants to ensure it is the right regulation. The issues facing the industry are complex, multi-faceted, and affect an important part of peoples' lives. As such, Facebook is absolutely committed to working with regulators, like Congress, to craft the right regulations. Facebook would be happy to review any proposed legislation and provide comments.

149. How do users benefit in anyway at all in having 3rd party people be privy to their private info?

We believe everyone deserves good privacy controls. A user owns the information they share on Facebook. This means they decide what they share and who they share it with on Facebook, and they can change their mind. We require websites and apps who use our tools to tell users they're collecting and sharing their information with us, and to get users' permission to do so.

Everyone has the right to expect strong protections for their information. We also need to do our part to help keep our community safe, in a way that's consistent with people's privacy expectations. We've recently announced several steps to give people more control over their privacy, including a new Privacy Shortcuts tool that we're rolling out now to give people information about how to control their information, including choosing who can see what they post and adding protections like two-factor authentication to their account. People can learn more about how to protect their privacy in our updated Data Policy and in our Privacy Basics feature (https://www.facebook.com/about/basics).

We are in the process of investigating every app that had access to a large amount of information before we changed our Platform in 2014. The investigation process is in full swing. We have large teams of internal and external experts working hard to investigate these apps as quickly as possible. As of early June 2018, thousands of apps have been investigated and around 200 apps have been suspended—pending a thorough investigation into whether they did in fact

misuse any data. Where we find evidence that these or other apps did misuse data, we will ban them and let people know.

Facebook is generally not opposed to regulation but wants to ensure it is the right regulation. The issues facing the industry are complex, multi-faceted, and affect an important part of peoples' lives. As such, Facebook is absolutely committed to working with regulators, like Congress, to craft the right regulations. Facebook would be happy to review any proposed legislation and provide comments.

150. When new privacy settings are added, why are they opt -in instead of opt -out?

We believe everyone deserves good privacy controls. A user owns the information they share on Facebook. This means they decide what they share and who they share it with on Facebook, and they can change their mind. We require websites and apps who use our tools to tell users they're collecting and sharing their information with us, and to get users' permission to do so.

Everyone has the right to expect strong protections for their information. We also need to do our part to help keep our community safe, in a way that's consistent with people's privacy expectations. We've recently announced several steps to give people more control over their privacy, including a new Privacy Shortcuts tool that we're rolling out now to give people information about how to control their information, including choosing who can see what they post and adding protections like two-factor authentication to their account. People can learn more about how to protect their privacy in our updated Data Policy and in our Privacy Basics feature (https://www.facebook.com/about/basics).

We are in the process of investigating every app that had access to a large amount of information before we changed our Platform in 2014. The investigation process is in full swing. We have large teams of internal and external experts working hard to investigate these apps as quickly as possible. As of early June 2018, thousands of apps have been investigated and around 200 apps have been suspended—pending a thorough investigation into whether they did in fact misuse any data. Where we find evidence that these or other apps did misuse data, we will ban them and let people know.

Facebook is generally not opposed to regulation but wants to ensure it is the right regulation. The issues facing the industry are complex, multi-faceted, and affect an important part of peoples' lives. As such, Facebook is absolutely committed to working with regulators, like Congress, to craft the right regulations. Facebook would be happy to review any proposed legislation and provide comments.

151. Why can't companies like Facebook take initiative in protecting users instead of waiting to be regulated by the government?

Protecting people's data is one of our most important responsibilities, and we are committed to continuing our work to improve how we protect people's information and to working with regulators to draft appropriate regulations. Our mission is to give people the power to build community and bring the world closer together. As the internet becomes more important in people's lives, the real question is about the right set of regulations that should apply to all

internet services, regardless of size. Across the board, we have a responsibility to not just build tools, but to make sure that they're used in ways that are positive for our users. Facebook is generally not opposed to regulation but wants to ensure it is the right regulation. The issues facing the industry are complex, multi-faceted, and affect an important part of peoples' lives. As such, Facebook is absolutely committed to working with regulators, like Congress, to craft the right regulations.

We are already regulated in many ways—for example, under the Federal Trade Commission Act—and we are subject to ongoing oversight by the FTC under the terms of a 2011 consent order. We furnished extensive information to the FTC regarding the ability for users to port their Facebook data (including friends data that had been shared with them) with apps on Facebook's platform, as part of the FTC's investigation culminating in the July 27, 2012 Consent Order. The Consent Order memorializes the agreement between Facebook and the FTC and did not require Facebook to turn off or change the ability for people to port friends data that had been shared with them on Facebook to apps they used. Facebook voluntarily changed this feature of Platform in 2014, however. Facebook has not violated the Federal Trade Commission Act. Facebook is not in a position to determine whether third-party app developers violated the Act and leaves that determination to the FTC, although we can confirm that misrepresenting the terms of an app to users is a violation of Facebook's developer policies.

Facebook has inherent incentives to protect its customers' privacy and address breaches and vulnerabilities. Indeed, the recent discovery of misconduct by an app developer on the Facebook platform clearly hurt Facebook and made it harder for us to achieve our social mission. As such, Facebook is committed to protecting our platform from bad actors, ensuring we are able to continue our mission of giving people a voice and bringing them closer together. It will take some time to work through all the changes we need to make across the company, but Facebook is committed to getting this right.

152. What measures will Facebook web designers do to ensure personal information be the property of users themselves to change and modify as those individuals see fit?

We believe that it's important to communicate with people about the information that we collect and how people can control it. As explained in our Data Policy, we collect three basic categories of data about people:

(1) data about things people do and share (and who they connect with) on our services;

(2) data about the devices people use to access our services; and

(3) data we receive from partners, including the websites and apps that use our business tools.

We collect information about the people, Pages, accounts, hashtags, and groups users are connected to and how they interact with them across our Products, such as people a user communicates with the most or groups users are part of. We also collect contact information if they choose to upload, sync, or import it from a device (such as an address book or call log or SMS log history), which we use for things like helping them and others find people they may know.

The data we use to show ads to people depends on the data we have received from people. For people who are new to Facebook, we may have minimal data that we can use. For people who have used our services for longer, we likely have more data, but the amount of data will depend on the nature of that use and how they have used our controls. Any person can see each of the specific interests we maintain about them for advertising by visiting Ads Preferences, which lets people see what interests we use to choose ads for them—and to edit or delete these interests. We also provide more detailed information about how we use data to decide what ads to show to people in our "About Facebook Ads" page, at https://www.facebook.com/ads/about. And, we do not sell people's information to anyone, and we never will.

All users must expressly consent to Facebook's Terms and Data Policy when registering for Facebook. The Data Policy explains the kinds of information we collect, how we use this information, how we share this information, and how users can manage and delete information.

Facebook does not create profiles for people without a Facebook account, but we do receive some information from devices and browsers that may be used by non-users. For example:

- When people visit apps or websites that feature our technologies—like the Facebook Like or Comment button—our servers automatically log (i) standard browser or app records of the fact that a particular device or user visited the website or app (this connection to Facebook's servers occurs automatically when a person visits a website or app that contains our technologies, such as a Like button, and is an inherent function of Internet design); and (ii) any additional information the publisher of the app or website chooses to share with Facebook about the person's activities on that site (such as the fact that a purchase was made on the site). This is a standard feature of the Internet, and most websites and apps share this same information with multiple different third-parties whenever people visit their website or app. When the person visiting a website featuring Facebook's tools is not a registered Facebook user, Facebook does not have information identifying that individual, and it does not create profiles for this individual.

- We also may receive information about the device of a non-registered user if that user visits a part of Facebook that does not require people to log in—such as a public Facebook Page. The information we log when people visit our websites or apps is the same as described above and is the same information that any provider of an online service would receive.

- In addition, Facebook may receive some basic information about devices where Facebook apps are installed, including before people using those devices have registered for Facebook (such as when a user downloads a Facebook app, but has not yet created an account, or if the app is preloaded on a given device). This device data includes things like device model, operating system, IP address, app version and device identifiers. We use this information to provide the right version of the app, help people who want to create accounts (for example, optimizing the registration flow for the specific device), retrieving bug fixes and measuring and improving app performance. We do not use this information to build profiles about non-registered users.

153. How can FB increase the transparency and authentication of account owners to avoid AI BOTS?

Claiming to be another person violates our Community Standards, and we want to make it harder for anyone to be impersonated on our platform, as well as more effectively detect and deactivate fake accounts to help reduce the spread of spam, false news, and misinformation.

We continually update our technical systems to identify, checkpoint, and remove inauthentic accounts, and we block millions of attempts to register fake accounts every day. As with all security threats, we have been incorporating new insights into our models for detecting fake accounts, including information specific to election issues. We've developed several techniques to help detect and block this type of abuse. At the time someone receives a friend request, our systems are designed to check whether the recipient already has a friend with the same name, along with a variety of other factors that help us determine if an interaction is legitimate. Further, we recently announced new features that use face recognition technology that may help detect when someone is using another user's image as their profile photo—which helps stop impersonation. Users can also report accounts that are impersonating them. This is an area we're continually working to improve so that we can provide a safe and secure experience on Facebook.

154. How can we find out if our personal data was scraped?

We believe everyone deserves good privacy controls. A user owns the information they share on Facebook. This means they decide what they share and who they share it with on Facebook, and they can change their mind. We require websites and apps who use our tools to tell users they're collecting and sharing their information with us, and to get users' permission to do so.

Everyone has the right to expect strong protections for their information. We also need to do our part to help keep our community safe, in a way that's consistent with people's privacy expectations. We've recently announced several steps to give people more control over their privacy, including a new Privacy Shortcuts tool that we're rolling out now to give people information about how to control their information, including choosing who can see what they post and adding protections like two-factor authentication to their account. People can learn more about how to protect their privacy in our updated Data Policy and in our Privacy Basics feature (https://www.facebook.com/about/basics).

We are in the process of investigating every app that had access to a large amount of information before we changed our Platform in 2014. The investigation process is in full swing. We have large teams of internal and external experts working hard to investigate these apps as quickly as possible. As of early June 2018, thousands of apps have been investigated and around 200 apps have been suspended—pending a thorough investigation into whether they did in fact misuse any data. Where we find evidence that these or other apps did misuse data, we will ban them and let people know.

Facebook is generally not opposed to regulation but wants to ensure it is the right regulation. The issues facing the industry are complex, multi-faceted, and affect an important

part of peoples' lives. As such, Facebook is absolutely committed to working with regulators, like Congress, to craft the right regulations. Facebook would be happy to review any proposed legislation and provide comments.

155. Hi. Thank you for soliciting our questions. As a Facebook customer I'd like to know if the customers will know they were breached and how we can be assured that our personal data is not being used currently or in the future for malicious purposes. What algorithm sent each end users data to Cambridge Analytica? Linda Miola Furrier Palo Alto, CA

Facebook's policies regarding third-party usage of its platform technologies have prohibited—and continue to prohibit—third-party app developers from selling or licensing user data accessed from Facebook and from sharing any user data accessed from Facebook with any ad network, data broker or other advertising or monetization-related service. We take action on potential violations of our Platform Policies based on proactive review, external reports, and other signals. Kogan was not permitted to sell or transfer data to third-parties for the purposes he did. In doing so, Kogan and his company violated Facebook's Platform Policies.

On December 11, 2015, *The Guardian* published an article reporting that Kogan and his company, GSR, may have passed information the app had obtained from Facebook users to SCL Elections Ltd. (SCL)/Cambridge Analytica. Facebook immediately banned Kogan's app from our platform and investigated what happened and what further action Facebook should take to enforce our Platform Policies. Facebook considered the matter closed after obtaining written certifications and confirmations from Kogan, GSR, Cambridge Analytica, and SCL declaring that all such data they had obtained was accounted for and destroyed. We did not have any reason to affirmatively question the veracity of any of these certifications until March 2018, when we learned from media reporting that questions had been raised concerning the accuracy of the certifications. Facebook immediately banned Cambridge Analytica and SCL from purchasing advertisements on our services as well as removed the personal accounts of some of their officers. Moreover, while Facebook's policies in place at the time allowed us to audit apps to ensure that they were safe and did not violate its terms, we had already terminated Kogan's app's access to Facebook. Accordingly, there were no ongoing concerns about the level of data that app could access or might access in the future. With the benefit of hindsight, we wish we had notified people whose information may have been impacted. Facebook has since notified all people potentially impacted with a detailed notice at the top of their News Feed.

156. Since interconnected personal information is continually being collected freely on Facebook's social network, what do you feel is Facebook's obligation to its community to provide transparency around what is being collected, and how and when this information is shared, and secondly, what are your thoughts around providing all Facebook users with the ability to request on-demand reports that detail what personal information is shared with who and when?

We believe that it's important to communicate with people about the information that we collect and how people can control it. As explained in our Data Policy, we collect three basic categories of data about people:

(1) data about things people do and share (and who they connect with) on our services;

(2) data about the devices people use to access our services; and

(3) data we receive from partners, including the websites and apps that use our business tools.

We collect information about the people, Pages, accounts, hashtags, and groups users are connected to and how they interact with them across our Products, such as people a user communicates with the most or groups users are part of. We also collect contact information if they choose to upload, sync, or import it from a device (such as an address book or call log or SMS log history), which we use for things like helping them and others find people they may know.

The data we use to show ads to people depends on the data we have received from people. For people who are new to Facebook, we may have minimal data that we can use. For people who have used our services for longer, we likely have more data, but the amount of data will depend on the nature of that use and how they have used our controls. Any person can see each of the specific interests we maintain about them for advertising by visiting Ads Preferences, which lets people see what interests we use to choose ads for them—and to edit or delete these interests. We also provide more detailed information about how we use data to decide what ads to show to people in our "About Facebook Ads" page, at https://www.facebook.com/ads/about. And, we do not sell people's information to anyone, and we never will.

All users must expressly consent to Facebook's Terms and Data Policy when registering for Facebook. The Data Policy explains the kinds of information we collect, how we use this information, how we share this information, and how users can manage and delete information.

Facebook does not create profiles for people without a Facebook account, but we do receive some information from devices and browsers that may be used by non-users. For example:

- When people visit apps or websites that feature our technologies—like the Facebook Like or Comment button—our servers automatically log (i) standard browser or app records of the fact that a particular device or user visited the website or app (this connection to Facebook's servers occurs automatically when a person visits a website or app that contains our technologies, such as a Like button, and is an inherent function of Internet design); and (ii) any additional information the publisher of the app or website chooses to share with Facebook about the person's activities on that site (such as the fact that a purchase was made on the site). This is a standard feature of the Internet, and most websites and apps share this same information with multiple different third-parties whenever people visit their website or app. When the person visiting a website featuring Facebook's tools is not a registered Facebook user, Facebook does not have information identifying that individual, and it does not create profiles for this individual.

- We also may receive information about the device of a non-registered user if that user visits a part of Facebook that does not require people to log in—such as a public

Facebook Page. The information we log when people visit our websites or apps is the same as described above and is the same information that any provider of an online service would receive.

- In addition, Facebook may receive some basic information about devices where Facebook apps are installed, including before people using those devices have registered for Facebook (such as when a user downloads a Facebook app, but has not yet created an account, or if the app is preloaded on a given device). This device data includes things like device model, operating system, IP address, app version and device identifiers. We use this information to provide the right version of the app, help people who want to create accounts (for example, optimizing the registration flow for the specific device), retrieving bug fixes and measuring and improving app performance. We do not use this information to build profiles about non-registered users.

157. When the environment on the internet is so hostile, and your business model is built specifically to harvest user data, how can you, over the long run, actually protect any data at all? Isn't the only real answer to turn control over every user's data completely back to them?

We believe everyone deserves good privacy controls. A user owns the information they share on Facebook. This means they decide what they share and who they share it with on Facebook, and they can change their mind. We require websites and apps who use our tools to tell users they're collecting and sharing their information with us, and to get users' permission to do so.

Everyone has the right to expect strong protections for their information. We also need to do our part to help keep our community safe, in a way that's consistent with people's privacy expectations. We've recently announced several steps to give people more control over their privacy, including a new Privacy Shortcuts tool that we're rolling out now to give people information about how to control their information, including choosing who can see what they post and adding protections like two-factor authentication to their account. People can learn more about how to protect their privacy in our updated Data Policy and in our Privacy Basics feature (https://www.facebook.com/about/basics).

We are in the process of investigating every app that had access to a large amount of information before we changed our Platform in 2014. The investigation process is in full swing. We have large teams of internal and external experts working hard to investigate these apps as quickly as possible. As of early June 2018, thousands of apps have been investigated and around 200 apps have been suspended—pending a thorough investigation into whether they did in fact misuse any data. Where we find evidence that these or other apps did misuse data, we will ban them and let people know.

Facebook is generally not opposed to regulation but wants to ensure it is the right regulation. The issues facing the industry are complex, multi-faceted, and affect an important part of peoples' lives. As such, Facebook is absolutely committed to working with regulators, like Congress, to craft the right regulations. Facebook would be happy to review any proposed legislation and provide comments.

158. Mr. Zuckerberg, has Facebook considered "dual factor" encryption, such as used by DOD and our national labs, to secure its digital reserves? Paul Grant

We believe everyone deserves good privacy controls. A user owns the information they share on Facebook. This means they decide what they share and who they share it with on Facebook, and they can change their mind. We require websites and apps who use our tools to tell users they're collecting and sharing their information with us, and to get users' permission to do so.

Everyone has the right to expect strong protections for their information. We also need to do our part to help keep our community safe, in a way that's consistent with people's privacy expectations. We've recently announced several steps to give people more control over their privacy, including a new Privacy Shortcuts tool that we're rolling out now to give people information about how to control their information, including choosing who can see what they post and adding protections like two-factor authentication to their account. People can learn more about how to protect their privacy in our updated Data Policy and in our Privacy Basics feature (https://www.facebook.com/about/basics).

We are in the process of investigating every app that had access to a large amount of information before we changed our Platform in 2014. The investigation process is in full swing. We have large teams of internal and external experts working hard to investigate these apps as quickly as possible. As of early June 2018, thousands of apps have been investigated and around 200 apps have been suspended—pending a thorough investigation into whether they did in fact misuse any data. Where we find evidence that these or other apps did misuse data, we will ban them and let people know.

Facebook is generally not opposed to regulation but wants to ensure it is the right regulation. The issues facing the industry are complex, multi-faceted, and affect an important part of peoples' lives. As such, Facebook is absolutely committed to working with regulators, like Congress, to craft the right regulations. Facebook would be happy to review any proposed legislation and provide comments.

159. How can you make it crystal clear what information is being shared with whom, and make it an Opt-In choice?

We believe everyone deserves good privacy controls. A user owns the information they share on Facebook. This means they decide what they share and who they share it with on Facebook, and they can change their mind. We require websites and apps who use our tools to tell users they're collecting and sharing their information with us, and to get users' permission to do so.

Everyone has the right to expect strong protections for their information. We also need to do our part to help keep our community safe, in a way that's consistent with people's privacy expectations. We've recently announced several steps to give people more control over their privacy, including a new Privacy Shortcuts tool that we're rolling out now to give people information about how to control their information, including choosing who can see what they post and adding protections like two-factor authentication to their account. People can learn more

about how to protect their privacy in our updated Data Policy and in our Privacy Basics feature (https://www.facebook.com/about/basics).

We are in the process of investigating every app that had access to a large amount of information before we changed our Platform in 2014. The investigation process is in full swing. We have large teams of internal and external experts working hard to investigate these apps as quickly as possible. As of early June 2018, thousands of apps have been investigated and around 200 apps have been suspended—pending a thorough investigation into whether they did in fact misuse any data. Where we find evidence that these or other apps did misuse data, we will ban them and let people know.

Facebook is generally not opposed to regulation but wants to ensure it is the right regulation. The issues facing the industry are complex, multi-faceted, and affect an important part of peoples' lives. As such, Facebook is absolutely committed to working with regulators, like Congress, to craft the right regulations. Facebook would be happy to review any proposed legislation and provide comments.

160. Is Facebook responsible for content, or is it a neutral platform like a telephone service provider?

Freedom of expression is one of our core values, and we believe that adding voices to the conversation creates a richer and more vibrant community. We want people to feel confident that our community welcomes all viewpoints and we are committed to designing our products to give all people a voice and foster the free flow of ideas and culture. We recognize how important it is for Facebook to be a place where people feel empowered to communicate, and we take our role in keeping abuse off our service seriously. Our mission entails embracing diverse views. We err on the side of allowing content, even when some find it objectionable, unless removing that content prevents a specific harm.

However, we are, first and foremost, a technology company. Facebook does not create or edit the content that our users post on our platform. While we seek to be a platform for a broad range of ideas, we do moderate content in good faith according to published community standards in order to keep users on the platform safe, reduce objectionable content and to make sure users participate on the platform responsibly.

161. Why does Facebook put up so much resistance to having one single page for privacy settings?

We believe everyone deserves good privacy controls. A user owns the information they share on Facebook. This means they decide what they share and who they share it with on Facebook, and they can change their mind. We require websites and apps who use our tools to tell users they're collecting and sharing their information with us, and to get users' permission to do so.

Everyone has the right to expect strong protections for their information. We also need to do our part to help keep our community safe, in a way that's consistent with people's privacy expectations. We've recently announced several steps to give people more control over their privacy, including a new Privacy Shortcuts tool that we're rolling out now to give people

information about how to control their information, including choosing who can see what they post and adding protections like two-factor authentication to their account. People can learn more about how to protect their privacy in our updated Data Policy and in our Privacy Basics feature (https://www.facebook.com/about/basics).

We are in the process of investigating every app that had access to a large amount of information before we changed our Platform in 2014. The investigation process is in full swing. We have large teams of internal and external experts working hard to investigate these apps as quickly as possible. As of early June 2018, thousands of apps have been investigated and around 200 apps have been suspended—pending a thorough investigation into whether they did in fact misuse any data. Where we find evidence that these or other apps did misuse data, we will ban them and let people know.

Facebook is generally not opposed to regulation but wants to ensure it is the right regulation. The issues facing the industry are complex, multi-faceted, and affect an important part of peoples' lives. As such, Facebook is absolutely committed to working with regulators, like Congress, to craft the right regulations. Facebook would be happy to review any proposed legislation and provide comments.

162. You've been repeatedly apologizing for Facebook's violations of its users' privacy since the company's founding-including signing a consent decree with the FTC in 2011. Why have you been consistently unable to correct or account for your inability to foresee the consequences of your decisions?

Protecting people's data is one of our most important responsibilities, and we are committed to continuing our work to improve how we protect people's information and to working with regulators to draft appropriate regulations. Our mission is to give people the power to build community and bring the world closer together. As the internet becomes more important in people's lives, the real question is about the right set of regulations that should apply to all internet services, regardless of size. Across the board, we have a responsibility to not just build tools, but to make sure that they're used in ways that are positive for our users. Facebook is generally not opposed to regulation but wants to ensure it is the right regulation. The issues facing the industry are complex, multi-faceted, and affect an important part of peoples' lives. As such, Facebook is absolutely committed to working with regulators, like Congress, to craft the right regulations.

We are already regulated in many ways—for example, under the Federal Trade Commission Act—and we are subject to ongoing oversight by the FTC under the terms of a 2011 consent order. We furnished extensive information to the FTC regarding the ability for users to port their Facebook data (including friends data that had been shared with them) with apps on Facebook's platform, as part of the FTC's investigation culminating in the July 27, 2012 Consent Order. The Consent Order memorializes the agreement between Facebook and the FTC and did not require Facebook to turn off or change the ability for people to port friends data that had been shared with them on Facebook to apps they used. Facebook voluntarily changed this feature of Platform in 2014, however. Facebook has not violated the Federal Trade Commission Act. Facebook is not in a position to determine whether third-party app developers violated the Act

and leaves that determination to the FTC, although we can confirm that misrepresenting the terms of an app to users is a violation of Facebook's developer policies.

Facebook has inherent incentives to protect its customers' privacy and address breaches and vulnerabilities. Indeed, the recent discovery of misconduct by an app developer on the Facebook platform clearly hurt Facebook and made it harder for us to achieve our social mission. As such, Facebook is committed to protecting our platform from bad actors, ensuring we are able to continue our mission of giving people a voice and bringing them closer together. It will take some time to work through all the changes we need to make across the company, but Facebook is committed to getting this right.

163. What assurances can you give the public that their data will not be accessed by unauthorized (by them) third parties?

Facebook's policies regarding third-party usage of its platform technologies have prohibited—and continue to prohibit—third-party app developers from selling or licensing user data obtained from Facebook and from sharing any user data obtained from Facebook with any ad network, data broker or other advertising or monetization-related service.

We use a variety of tools to enforce Facebook policies against violating parties, including developers. We review tens of thousands of apps per year and regularly disapprove noncompliant apps as part of our proactive review process. We also use tools like cease and desist letters, account suspensions, letter agreements, and civil litigation. For example, since 2006, Facebook has sent over 1,150 cease-and-desist letters to over 1,600 targets. In 2017, we took action against about 370,000 apps, ranging from imposing certain restrictions to removal of the app from the platform. Moreover, we have required parties who have procured our data without authorization to delete that data. We have invested significant resources in these efforts.

Recently, we announced a number of additional steps we're taking to address concerns raised by Kogan's app.

1. **Review our platform.** We will investigate all apps that had access to large amounts of data before the platform changes we announced in 2014, and we will audit any app where we identify suspicious activity. If we identify misuses of data, we'll take immediate action, including banning the app from our platform and pursuing legal action if appropriate.

2. **Tell people about data misuse.** We will tell people about apps that have misused their data. This includes building a way for people to know if their data might have been accessed via the app. Moving forward, if we remove an app, we will tell people.

3. **Turn off access for unused apps.** If someone has not used an app within the last three months, we will turn off the app's access to their data.

4. **Restrict Facebook Login data.** We are changing Login, so that the only data that an app can request without app review will include name, profile photo, and email address. Requesting any other data will require approval from Facebook. We will also no longer allow apps to ask for access to information like religious or political views,

relationship status and details, custom friends lists, education and work history, fitness activity, book reading and music listening activity, news reading, video watch activity, and games activity. We will encourage people to manage the apps they use. We already show people what apps their accounts are connected to and allow them to control what data they've permitted those apps to use. But we're making it easier for people to see what apps they use and the information they have shared with those apps.

5. **Reward people who find vulnerabilities.** We launched the Data Abuse Bounty program so that people can report to us any misuses of data by app developers.

6. **Update our policies.** We have updated our terms and Data Policy to explain how we use data and how data is shared with app developers.

164. Please discuss why FB did not comply with the 2011 consent decree requirements?

Protecting people's data is one of our most important responsibilities, and we are committed to continuing our work to improve how we protect people's information and to working with regulators to draft appropriate regulations. Our mission is to give people the power to build community and bring the world closer together. As the internet becomes more important in people's lives, the real question is about the right set of regulations that should apply to all internet services, regardless of size. Across the board, we have a responsibility to not just build tools, but to make sure that they're used in ways that are positive for our users. Facebook is generally not opposed to regulation but wants to ensure it is the right regulation. The issues facing the industry are complex, multi-faceted, and affect an important part of peoples' lives. As such, Facebook is absolutely committed to working with regulators, like Congress, to craft the right regulations.

We are already regulated in many ways—for example, under the Federal Trade Commission Act—and we are subject to ongoing oversight by the FTC under the terms of a 2011 consent order. We furnished extensive information to the FTC regarding the ability for users to port their Facebook data (including friends data that had been shared with them) with apps on Facebook's platform, as part of the FTC's investigation culminating in the July 27, 2012 Consent Order. The Consent Order memorializes the agreement between Facebook and the FTC and did not require Facebook to turn off or change the ability for people to port friends data that had been shared with them on Facebook to apps they used. Facebook voluntarily changed this feature of Platform in 2014, however. Facebook has not violated the Federal Trade Commission Act. Facebook is not in a position to determine whether third-party app developers violated the Act and leaves that determination to the FTC, although we can confirm that misrepresenting the terms of an app to users is a violation of Facebook's developer policies.

Facebook has inherent incentives to protect its customers' privacy and address breaches and vulnerabilities. Indeed, the recent discovery of misconduct by an app developer on the Facebook platform clearly hurt Facebook and made it harder for us to achieve our social mission. As such, Facebook is committed to protecting our platform from bad actors, ensuring we are able to continue our mission of giving people a voice and bringing them closer together. It will take

some time to work through all the changes we need to make across the company, but Facebook is committed to getting this right.

165. How may I help you protect our data and identity information?

We believe everyone deserves good privacy controls. A user owns the information they share on Facebook. This means they decide what they share and who they share it with on Facebook, and they can change their mind. We require websites and apps who use our tools to tell users they're collecting and sharing their information with us, and to get users' permission to do so.

Everyone has the right to expect strong protections for their information. We also need to do our part to help keep our community safe, in a way that's consistent with people's privacy expectations. We've recently announced several steps to give people more control over their privacy, including a new Privacy Shortcuts tool that we're rolling out now to give people information about how to control their information, including choosing who can see what they post and adding protections like two-factor authentication to their account. People can learn more about how to protect their privacy in our updated Data Policy and in our Privacy Basics feature (https://www.facebook.com/about/basics).

We are in the process of investigating every app that had access to a large amount of information before we changed our Platform in 2014. The investigation process is in full swing. We have large teams of internal and external experts working hard to investigate these apps as quickly as possible. As of early June 2018, thousands of apps have been investigated and around 200 apps have been suspended—pending a thorough investigation into whether they did in fact misuse any data. Where we find evidence that these or other apps did misuse data, we will ban them and let people know.

Facebook is generally not opposed to regulation but wants to ensure it is the right regulation. The issues facing the industry are complex, multi-faceted, and affect an important part of peoples' lives. As such, Facebook is absolutely committed to working with regulators, like Congress, to craft the right regulations. Facebook would be happy to review any proposed legislation and provide comments.

166. How does Facebook plan to implement protections to user data in its application, and how will these changes be communicated to account users in a user-friendly way?

We believe everyone deserves good privacy controls. A user owns the information they share on Facebook. This means they decide what they share and who they share it with on Facebook, and they can change their mind. We require websites and apps who use our tools to tell users they're collecting and sharing their information with us, and to get users' permission to do so.

Everyone has the right to expect strong protections for their information. We also need to do our part to help keep our community safe, in a way that's consistent with people's privacy expectations. We've recently announced several steps to give people more control over their privacy, including a new Privacy Shortcuts tool that we're rolling out now to give people

information about how to control their information, including choosing who can see what they post and adding protections like two-factor authentication to their account. People can learn more about how to protect their privacy in our updated Data Policy and in our Privacy Basics feature (https://www.facebook.com/about/basics).

We are in the process of investigating every app that had access to a large amount of information before we changed our Platform in 2014. The investigation process is in full swing. We have large teams of internal and external experts working hard to investigate these apps as quickly as possible. As of early June 2018, thousands of apps have been investigated and around 200 apps have been suspended—pending a thorough investigation into whether they did in fact misuse any data. Where we find evidence that these or other apps did misuse data, we will ban them and let people know.

Facebook is generally not opposed to regulation but wants to ensure it is the right regulation. The issues facing the industry are complex, multi-faceted, and affect an important part of peoples' lives. As such, Facebook is absolutely committed to working with regulators, like Congress, to craft the right regulations. Facebook would be happy to review any proposed legislation and provide comments.

167. Is there a way Facebook can allow users to share their data with individuals but prevent automated data harvesting robots from getting the data?

Facebook's policies regarding third-party usage of its platform technologies have prohibited—and continue to prohibit—third-party app developers from selling or licensing user data obtained from Facebook and from sharing any user data obtained from Facebook with any ad network, data broker or other advertising or monetization-related service.

We use a variety of tools to enforce Facebook policies against violating parties, including developers. We review tens of thousands of apps per year and regularly disapprove noncompliant apps as part of our proactive review process. We also use tools like cease and desist letters, account suspensions, letter agreements, and civil litigation. For example, since 2006, Facebook has sent over 1,150 cease-and-desist letters to over 1,600 targets. In 2017, we took action against about 370,000 apps, ranging from imposing certain restrictions to removal of the app from the platform. Moreover, we have required parties who have procured our data without authorization to delete that data. We have invested significant resources in these efforts.

Recently, we announced a number of additional steps we're taking to address concerns raised by Kogan's app.

7. **Review our platform.** We will investigate all apps that had access to large amounts of data before the platform changes we announced in 2014, and we will audit any app where we identify suspicious activity. If we identify misuses of data, we'll take immediate action, including banning the app from our platform and pursuing legal action if appropriate.

8. **Tell people about data misuse.** We will tell people about apps that have misused their data. This includes building a way for people to know if their data might have been accessed via the app. Moving forward, if we remove an app, we will tell people.

9. **Turn off access for unused apps.** If someone has not used an app within the last three months, we will turn off the app's access to their data.

10. **Restrict Facebook Login data.** We are changing Login, so that the only data that an app can request without app review will include name, profile photo, and email address. Requesting any other data will require approval from Facebook. We will also no longer allow apps to ask for access to information like religious or political views, relationship status and details, custom friends lists, education and work history, fitness activity, book reading and music listening activity, news reading, video watch activity, and games activity. We will encourage people to manage the apps they use. We already show people what apps their accounts are connected to and allow them to control what data they've permitted those apps to use. But we're making it easier for people to see what apps they use and the information they have shared with those apps.

11. **Reward people who find vulnerabilities.** We launched the Data Abuse Bounty program so that people can report to us any misuses of data by app developers.

12. **Update our policies.** We have updated our terms and Data Policy to explain how we use data and how data is shared with app developers.

168. Who legally owns the data that is posted on Facebook? The individual posting it or Facebook?

We believe everyone deserves good privacy controls. A user owns the information they share on Facebook. This means they decide what they share and who they share it with on Facebook, and they can change their mind. We require websites and apps who use our tools to tell users they're collecting and sharing their information with us, and to get users' permission to do so.

Everyone has the right to expect strong protections for their information. We also need to do our part to help keep our community safe, in a way that's consistent with people's privacy expectations. We've recently announced several steps to give people more control over their privacy, including a new Privacy Shortcuts tool that we're rolling out now to give people information about how to control their information, including choosing who can see what they post and adding protections like two-factor authentication to their account. People can learn more about how to protect their privacy in our updated Data Policy and in our Privacy Basics feature (https://www.facebook.com/about/basics).

We are in the process of investigating every app that had access to a large amount of information before we changed our Platform in 2014. The investigation process is in full swing. We have large teams of internal and external experts working hard to investigate these apps as quickly as possible. As of early June 2018, thousands of apps have been investigated and around 200 apps have been suspended—pending a thorough investigation into whether they did in fact misuse any data. Where we find evidence that these or other apps did misuse data, we will ban them and let people know.

Facebook is generally not opposed to regulation but wants to ensure it is the right regulation. The issues facing the industry are complex, multi-faceted, and affect an important part of peoples' lives. As such, Facebook is absolutely committed to working with regulators, like Congress, to craft the right regulations. Facebook would be happy to review any proposed legislation and provide comments.

169. Mr. Zuckerberg, in "joining people together" did Facebook, in your opinion, adequately protect users from advertisers? Flow is it that Facebook believed it had the right to sell user information without informing them, or obtaining user consent?

To build a secure product with extensive infrastructure that connects people wherever they live or whatever their income level, we need to make sure everyone can afford it. Advertising lets us keep Facebook free, which ensures it remains affordable for everyone. We also believe the ads you see across the Facebook family of apps and services should be useful and relevant to you. Users can't opt out of seeing ads altogether because selling ads is what keeps Facebook free, but they do have different options to control how their data can and can't be used to show them ads. They're all found in ad preferences, which allows users to turn off the use of all data collected from partners off Facebook to target ads. Users can also decide which of their profile fields they want used for ad targeting in the Information section under "About you." Users can remove themselves from interests under "Your interests" and categories under "Your categories." And, we do not sell people's information to anyone, and we never will.

Facebook is committed to transparency for all ads, including ads with political content. Facebook believes that people should be able to easily understand why they are seeing ads, who paid for them, and what other ads those advertisers are running. As such, Facebook only allows authorized advertisers to run ads about elections or issues that are being debated across the country. In order to be authorized by Facebook, advertisers will need to confirm their identity and location. Furthermore, all political and issue ads will include a disclosure which reads: "Paid for by," and when users click on this disclosure they will be able to see details about the advertiser. Users will also be able to see an explanation of why they saw the particular ad. This is similar to the disclosure included on political TV advertisements. We just launched globally View Active Ads, a feature that will enable anyone to see all of the ads an advertiser is currently running by visiting the advertiser's Facebook Page.

170. Why won't you commit to extending to US citizens the privacy protections extended to EU citizens?

As a part of our overall approach to privacy, we are providing the same tools for access, rectification, erasure, data portability and others to people in the US (and globally) that we provide in the European Union under the GDPR. The controls and settings that Facebook is enabling as part of GDPR include settings for controlling our use of face recognition on Facebook and for controlling our ability to use data we collect off Facebook Company Products to target ads. We recently began providing direct notice of these controls and our updated terms to people around the world (including in the US), allowing people to choose whether or not to enable or disable these settings or to consent to our updated terms. Many of these tools (like our

Download Your Information tool, ad preferences tool, and Activity Log) have been available globally for many years.

However, the GDPR creates some specific requirements that do not apply in the rest of the world, for example the requirement to provide contact information for the EU Data Protection Officer or to specify legal bases for processing data. We are also looking to be more responsive to regional norms and legal frameworks going forward, and want to have the flexibility to work with local regulators, which is possible with this new model. At the same time, we are changing the provisions in our Facebook, Inc. terms in our user agreements outside the United States to allow people in other countries to file lawsuits against Facebook in their home country,

171. Why does Facebook need to harvest my personal information? Isn't your advertising enough?

We believe that it's important to communicate with people about the information that we collect and how people can control it. As explained in our Data Policy, we collect three basic categories of data about people:

(1) data about things people do and share (and who they connect with) on our services;

(2) data about the devices people use to access our services; and

(3) data we receive from partners, including the websites and apps that use our business tools.

We collect information about the people, Pages, accounts, hashtags, and groups users are connected to and how they interact with them across our Products, such as people a user communicates with the most or groups users are part of. We also collect contact information if they choose to upload, sync, or import it from a device (such as an address book or call log or SMS log history), which we use for things like helping them and others find people they may know.

The data we use to show ads to people depends on the data we have received from people. For people who are new to Facebook, we may have minimal data that we can use. For people who have used our services for longer, we likely have more data, but the amount of data will depend on the nature of that use and how they have used our controls. Any person can see each of the specific interests we maintain about them for advertising by visiting Ads Preferences, which lets people see what interests we use to choose ads for them—and to edit or delete these interests. We also provide more detailed information about how we use data to decide what ads to show to people in our "About Facebook Ads" page, at https://www.facebook.com/ads/about. And, we do not sell people's information to anyone, and we never will.

All users must expressly consent to Facebook's Terms and Data Policy when registering for Facebook. The Data Policy explains the kinds of information we collect, how we use this information, how we share this information, and how users can manage and delete information.

Facebook does not create profiles for people without a Facebook account, but we do receive some information from devices and browsers that may be used by non-users. For example:

- When people visit apps or websites that feature our technologies—like the Facebook Like or Comment button—our servers automatically log (i) standard browser or app records of the fact that a particular device or user visited the website or app (this connection to Facebook's servers occurs automatically when a person visits a website or app that contains our technologies, such as a Like button, and is an inherent function of Internet design); and (ii) any additional information the publisher of the app or website chooses to share with Facebook about the person's activities on that site (such as the fact that a purchase was made on the site). This is a standard feature of the Internet, and most websites and apps share this same information with multiple different third-parties whenever people visit their website or app. When the person visiting a website featuring Facebook's tools is not a registered Facebook user, Facebook does not have information identifying that individual, and it does not create profiles for this individual.

- We also may receive information about the device of a non-registered user if that user visits a part of Facebook that does not require people to log in—such as a public Facebook Page. The information we log when people visit our websites or apps is the same as described above and is the same information that any provider of an online service would receive.

- In addition, Facebook may receive some basic information about devices where Facebook apps are installed, including before people using those devices have registered for Facebook (such as when a user downloads a Facebook app, but has not yet created an account, or if the app is preloaded on a given device). This device data includes things like device model, operating system, IP address, app version and device identifiers. We use this information to provide the right version of the app, help people who want to create accounts (for example, optimizing the registration flow for the specific device), retrieving bug fixes and measuring and improving app performance. We do not use this information to build profiles about non-registered users.

172. The EU says consumers own their information, do you believe consumers own their data about their likes and preferences?

As a part of our overall approach to privacy, we are providing the same tools for access, rectification, erasure, data portability and others to people in the US (and globally) that we provide in the European Union under the GDPR. The controls and settings that Facebook is enabling as part of GDPR include settings for controlling our use of face recognition on Facebook and for controlling our ability to use data we collect off Facebook Company Products to target ads. We recently began providing direct notice of these controls and our updated terms to people around the world (including in the US), allowing people to choose whether or not to enable or disable these settings or to consent to our updated terms. Many of these tools (like our Download Your Information tool, ad preferences tool, and Activity Log) have been available globally for many years.

However, the GDPR creates some specific requirements that do not apply in the rest of the world, for example the requirement to provide contact information for the EU Data Protection Officer or to specify legal bases for processing data. We are also looking to be more responsive to regional norms and legal frameworks going forward, and want to have the flexibility to work with local regulators, which is possible with this new model. At the same time, we are changing the provisions in our Facebook, Inc. terms in our user agreements outside the United States to allow people in other countries to file lawsuits against Facebook in their home country, rather than in courts in the US. This transition was part of a continued effort to be locally responsive in countries where people use our services.

173. I thought that information collected by FB or an App, would be general, telling something like guys preferred black ties with polka dots so manufacturers could make them and sell them like hot cakes. When did it switch so that the data collectors knew who in particular liked the poker dot ties? And why?

Facebook's policies regarding third-party usage of its platform technologies have prohibited—and continue to prohibit—third-party app developers from selling or licensing user data obtained from Facebook and from sharing any user data obtained from Facebook with any ad network, data broker or other advertising or monetization-related service.

We use a variety of tools to enforce Facebook policies against violating parties, including developers. We review tens of thousands of apps per year and regularly disapprove noncompliant apps as part of our proactive review process. We also use tools like cease and desist letters, account suspensions, letter agreements, and civil litigation. For example, since 2006, Facebook has sent over 1,150 cease-and-desist letters to over 1,600 targets. In 2017, we took action against about 370,000 apps, ranging from imposing certain restrictions to removal of the app from the platform. Moreover, we have required parties who have procured our data without authorization to delete that data. We have invested significant resources in these efforts.

Recently, we announced a number of additional steps we're taking to address concerns raised by Kogan's app.

13. **Review our platform.** We will investigate all apps that had access to large amounts of data before the platform changes we announced in 2014, and we will audit any app where we identify suspicious activity. If we identify misuses of data, we'll take immediate action, including banning the app from our platform and pursuing legal action if appropriate.

14. **Tell people about data misuse.** We will tell people about apps that have misused their data. This includes building a way for people to know if their data might have been accessed via the app. Moving forward, if we remove an app, we will tell people.

15. **Turn off access for unused apps.** If someone has not used an app within the last three months, we will turn off the app's access to their data.

16. **Restrict Facebook Login data.** We are changing Login, so that the only data that an app can request without app review will include name, profile photo, and email address. Requesting any other data will require approval from Facebook. We will also

no longer allow apps to ask for access to information like religious or political views, relationship status and details, custom friends lists, education and work history, fitness activity, book reading and music listening activity, news reading, video watch activity, and games activity. We will encourage people to manage the apps they use. We already show people what apps their accounts are connected to and allow them to control what data they've permitted those apps to use. But we're making it easier for people to see what apps they use and the information they have shared with those apps.

17. **Reward people who find vulnerabilities.** We launched the Data Abuse Bounty program so that people can report to us any misuses of data by app developers.

18. **Update our policies.** We have updated our terms and Data Policy to explain how we use data and how data is shared with app developers.

174. Will you allow your users to remove data they consider private? When?

We believe everyone deserves good privacy controls. A user owns the information they share on Facebook. This means they decide what they share and who they share it with on Facebook, and they can change their mind. We require websites and apps who use our tools to tell users they're collecting and sharing their information with us, and to get users' permission to do so.

Everyone has the right to expect strong protections for their information. We also need to do our part to help keep our community safe, in a way that's consistent with people's privacy expectations. We've recently announced several steps to give people more control over their privacy, including a new Privacy Shortcuts tool that we're rolling out now to give people information about how to control their information, including choosing who can see what they post and adding protections like two-factor authentication to their account. People can learn more about how to protect their privacy in our updated Data Policy and in our Privacy Basics feature (https://www.facebook.com/about/basics).

We are in the process of investigating every app that had access to a large amount of information before we changed our Platform in 2014. The investigation process is in full swing. We have large teams of internal and external experts working hard to investigate these apps as quickly as possible. As of early June 2018, thousands of apps have been investigated and around 200 apps have been suspended—pending a thorough investigation into whether they did in fact misuse any data. Where we find evidence that these or other apps did misuse data, we will ban them and let people know.

Facebook is generally not opposed to regulation but wants to ensure it is the right regulation. The issues facing the industry are complex, multi-faceted, and affect an important part of peoples' lives. As such, Facebook is absolutely committed to working with regulators, like Congress, to craft the right regulations. Facebook would be happy to review any proposed legislation and provide comments.

175. If Facebook aware of other third-party information mishandlings that they have not disclosed?

Facebook's policies regarding third-party usage of its platform technologies have prohibited—and continue to prohibit—third-party app developers from selling or licensing user data obtained from Facebook and from sharing any user data obtained from Facebook with any ad network, data broker or other advertising or monetization-related service.

We use a variety of tools to enforce Facebook policies against violating parties, including developers. We review tens of thousands of apps per year and regularly disapprove noncompliant apps as part of our proactive review process. We also use tools like cease and desist letters, account suspensions, letter agreements, and civil litigation. For example, since 2006, Facebook has sent over 1,150 cease-and-desist letters to over 1,600 targets. In 2017, we took action against about 370,000 apps, ranging from imposing certain restrictions to removal of the app from the platform. Moreover, we have required parties who have procured our data without authorization to delete that data. We have invested significant resources in these efforts.

Recently, we announced a number of additional steps we're taking to address concerns raised by Kogan's app.

19. **Review our platform.** We will investigate all apps that had access to large amounts of data before the platform changes we announced in 2014, and we will audit any app where we identify suspicious activity. If we identify misuses of data, we'll take immediate action, including banning the app from our platform and pursuing legal action if appropriate.

20. **Tell people about data misuse.** We will tell people about apps that have misused their data. This includes building a way for people to know if their data might have been accessed via the app. Moving forward, if we remove an app, we will tell people.

21. **Turn off access for unused apps.** If someone has not used an app within the last three months, we will turn off the app's access to their data.

22. **Restrict Facebook Login data.** We are changing Login, so that the only data that an app can request without app review will include name, profile photo, and email address. Requesting any other data will require approval from Facebook. We will also no longer allow apps to ask for access to information like religious or political views, relationship status and details, custom friends lists, education and work history, fitness activity, book reading and music listening activity, news reading, video watch activity, and games activity. We will encourage people to manage the apps they use. We already show people what apps their accounts are connected to and allow them to control what data they've permitted those apps to use. But we're making it easier for people to see what apps they use and the information they have shared with those apps.

23. **Reward people who find vulnerabilities.** We launched the Data Abuse Bounty program so that people can report to us any misuses of data by app developers.

24. **Update our policies.** We have updated our terms and Data Policy to explain how we use data and how data is shared with app developers.

176. User privacy and advertising ease are sometimes in tension. Will you commit to consistently privilege user privacy over advertising ease, and exactly how?

To build a secure product with extensive infrastructure that connects people wherever they live or whatever their income level, we need to make sure everyone can afford it. Advertising lets us keep Facebook free, which ensures it remains affordable for everyone. We also believe the ads you see across the Facebook family of apps and services should be useful and relevant to you. Users can't opt out of seeing ads altogether because selling ads is what keeps Facebook free, but they do have different options to control how their data can and can't be used to show them ads. They're all found in ad preferences, which allows users to turn off the use of all data collected from partners off Facebook to target ads. Users can also decide which of their profile fields they want used for ad targeting in the Information section under "About you." Users can remove themselves from interests under "Your interests" and categories under "Your categories." And, we do not sell people's information to anyone, and we never will.

Facebook is committed to transparency for all ads, including ads with political content. Facebook believes that people should be able to easily understand why they are seeing ads, who paid for them, and what other ads those advertisers are running. As such, Facebook only allows authorized advertisers to run ads about elections or issues that are being debated across the country. In order to be authorized by Facebook, advertisers will need to confirm their identity and location. Furthermore, all political and issue ads will include a disclosure which reads: "Paid for by," and when users click on this disclosure they will be able to see details about the advertiser. Users will also be able to see an explanation of why they saw the particular ad. This is similar to the disclosure included on political TV advertisements. We just launched globally View Active Ads, a feature that will enable anyone to see all of the ads an advertiser is currently running by visiting the advertiser's Facebook Page.

177. Facebook requires users to provide email and cellphone numbers. The latter are used for two-factor authentication. FB has monetized security information. Is this a good idea?

We believe that it's important to communicate with people about the information that we collect and how people can control it. As explained in our Data Policy, we collect three basic categories of data about people:

(1) data about things people do and share (and who they connect with) on our services;

(2) data about the devices people use to access our services; and

(3) data we receive from partners, including the websites and apps that use our business tools.

We collect information about the people, Pages, accounts, hashtags, and groups users are connected to and how they interact with them across our Products, such as people a user communicates with the most or groups users are part of. We also collect contact information if they choose to upload, sync, or import it from a device (such as an address book or call log or SMS log history), which we use for things like helping them and others find people they may know.

The data we use to show ads to people depends on the data we have received from people. For people who are new to Facebook, we may have minimal data that we can use. For people who have used our services for longer, we likely have more data, but the amount of data will depend on the nature of that use and how they have used our controls. Any person can see each of the specific interests we maintain about them for advertising by visiting Ads Preferences, which lets people see what interests we use to choose ads for them—and to edit or delete these interests. We also provide more detailed information about how we use data to decide what ads to show to people in our "About Facebook Ads" page, at https://www.facebook.com/ads/about. And, we do not sell people's information to anyone, and we never will.

All users must expressly consent to Facebook's Terms and Data Policy when registering for Facebook. The Data Policy explains the kinds of information we collect, how we use this information, how we share this information, and how users can manage and delete information.

Facebook does not create profiles for people without a Facebook account, but we do receive some information from devices and browsers that may be used by non-users. For example:

- When people visit apps or websites that feature our technologies—like the Facebook Like or Comment button—our servers automatically log (i) standard browser or app records of the fact that a particular device or user visited the website or app (this connection to Facebook's servers occurs automatically when a person visits a website or app that contains our technologies, such as a Like button, and is an inherent function of Internet design); and (ii) any additional information the publisher of the app or website chooses to share with Facebook about the person's activities on that site (such as the fact that a purchase was made on the site). This is a standard feature of the Internet, and most websites and apps share this same information with multiple different third-parties whenever people visit their website or app. When the person visiting a website featuring Facebook's tools is not a registered Facebook user, Facebook does not have information identifying that individual, and it does not create profiles for this individual.

- We also may receive information about the device of a non-registered user if that user visits a part of Facebook that does not require people to log in—such as a public Facebook Page. The information we log when people visit our websites or apps is the same as described above and is the same information that any provider of an online service would receive.

- In addition, Facebook may receive some basic information about devices where Facebook apps are installed, including before people using those devices have registered for Facebook (such as when a user downloads a Facebook app, but has not yet created an account, or if the app is preloaded on a given device). This device data includes things like device model, operating system, IP address, app version and device identifiers. We use this information to provide the right version of the app, help people who want to create accounts (for example, optimizing the registration flow for the specific device), retrieving bug fixes and measuring and improving app performance. We do not use this information to build profiles about non-registered users.

178. How can I control my personal data on Facebook?

We believe everyone deserves good privacy controls. A user owns the information they share on Facebook. This means they decide what they share and who they share it with on Facebook, and they can change their mind. We require websites and apps who use our tools to tell users they're collecting and sharing their information with us, and to get users' permission to do so.

Everyone has the right to expect strong protections for their information. We also need to do our part to help keep our community safe, in a way that's consistent with people's privacy expectations. We've recently announced several steps to give people more control over their privacy, including a new Privacy Shortcuts tool that we're rolling out now to give people information about how to control their information, including choosing who can see what they post and adding protections like two-factor authentication to their account. People can learn more about how to protect their privacy in our updated Data Policy and in our Privacy Basics feature (https://www.facebook.com/about/basics).

We are in the process of investigating every app that had access to a large amount of information before we changed our Platform in 2014. The investigation process is in full swing. We have large teams of internal and external experts working hard to investigate these apps as quickly as possible. As of early June 2018, thousands of apps have been investigated and around 200 apps have been suspended—pending a thorough investigation into whether they did in fact misuse any data. Where we find evidence that these or other apps did misuse data, we will ban them and let people know.

Facebook is generally not opposed to regulation but wants to ensure it is the right regulation. The issues facing the industry are complex, multi-faceted, and affect an important part of peoples' lives. As such, Facebook is absolutely committed to working with regulators, like Congress, to craft the right regulations. Facebook would be happy to review any proposed legislation and provide comments.

179. Will your company make privacy easier for the consumer to understand and use so they do not have to be concerned about their personal information?

We believe everyone deserves good privacy controls. A user owns the information they share on Facebook. This means they decide what they share and who they share it with on Facebook, and they can change their mind. We require websites and apps who use our tools to tell users they're collecting and sharing their information with us, and to get users' permission to do so.

Everyone has the right to expect strong protections for their information. We also need to do our part to help keep our community safe, in a way that's consistent with people's privacy expectations. We've recently announced several steps to give people more control over their privacy, including a new Privacy Shortcuts tool that we're rolling out now to give people information about how to control their information, including choosing who can see what they post and adding protections like two-factor authentication to their account. People can learn more about how to protect their privacy in our updated Data Policy and in our Privacy Basics feature (https://www.facebook.com/about/basics).

We are in the process of investigating every app that had access to a large amount of information before we changed our Platform in 2014. The investigation process is in full swing. We have large teams of internal and external experts working hard to investigate these apps as quickly as possible. As of early June 2018, thousands of apps have been investigated and around 200 apps have been suspended—pending a thorough investigation into whether they did in fact misuse any data. Where we find evidence that these or other apps did misuse data, we will ban them and let people know.

Facebook is generally not opposed to regulation but wants to ensure it is the right regulation. The issues facing the industry are complex, multi-faceted, and affect an important part of peoples' lives. As such, Facebook is absolutely committed to working with regulators, like Congress, to craft the right regulations. Facebook would be happy to review any proposed legislation and provide comments.

180. Shouldn't Facebook make users decisions on privacy decisions OPT-IN, not OPT OUT

We believe everyone deserves good privacy controls. A user owns the information they share on Facebook. This means they decide what they share and who they share it with on Facebook, and they can change their mind. We require websites and apps who use our tools to tell users they're collecting and sharing their information with us, and to get users' permission to do so.

Everyone has the right to expect strong protections for their information. We also need to do our part to help keep our community safe, in a way that's consistent with people's privacy expectations. We've recently announced several steps to give people more control over their privacy, including a new Privacy Shortcuts tool that we're rolling out now to give people information about how to control their information, including choosing who can see what they post and adding protections like two-factor authentication to their account. People can learn more about how to protect their privacy in our updated Data Policy and in our Privacy Basics feature (https://www.facebook.com/about/basics).

We are in the process of investigating every app that had access to a large amount of information before we changed our Platform in 2014. The investigation process is in full swing. We have large teams of internal and external experts working hard to investigate these apps as quickly as possible. As of early June 2018, thousands of apps have been investigated and around 200 apps have been suspended—pending a thorough investigation into whether they did in fact misuse any data. Where we find evidence that these or other apps did misuse data, we will ban them and let people know.

Facebook is generally not opposed to regulation but wants to ensure it is the right regulation. The issues facing the industry are complex, multi-faceted, and affect an important part of peoples' lives. As such, Facebook is absolutely committed to working with regulators, like Congress, to craft the right regulations. Facebook would be happy to review any proposed legislation and provide comments.

181. Why isn't my privacy a top priority?

We believe everyone deserves good privacy controls. A user owns the information they share on Facebook. This means they decide what they share and who they share it with on Facebook, and they can change their mind. We require websites and apps who use our tools to tell users they're collecting and sharing their information with us, and to get users' permission to do so.

Everyone has the right to expect strong protections for their information. We also need to do our part to help keep our community safe, in a way that's consistent with people's privacy expectations. We've recently announced several steps to give people more control over their privacy, including a new Privacy Shortcuts tool that we're rolling out now to give people information about how to control their information, including choosing who can see what they post and adding protections like two-factor authentication to their account. People can learn more about how to protect their privacy in our updated Data Policy and in our Privacy Basics feature (https://www.facebook.com/about/basics).

We are in the process of investigating every app that had access to a large amount of information before we changed our Platform in 2014. The investigation process is in full swing. We have large teams of internal and external experts working hard to investigate these apps as quickly as possible. As of early June 2018, thousands of apps have been investigated and around 200 apps have been suspended—pending a thorough investigation into whether they did in fact misuse any data. Where we find evidence that these or other apps did misuse data, we will ban them and let people know.

Facebook is generally not opposed to regulation but wants to ensure it is the right regulation. The issues facing the industry are complex, multi-faceted, and affect an important part of peoples' lives. As such, Facebook is absolutely committed to working with regulators, like Congress, to craft the right regulations. Facebook would be happy to review any proposed legislation and provide comments.

182. If Facebook continues to be free, what am I giving up for this service

We believe that it's important to communicate with people about the information that we collect and how people can control it. As explained in our Data Policy, we collect three basic categories of data about people:

(1) data about things people do and share (and who they connect with) on our services;

(2) data about the devices people use to access our services; and

(3) data we receive from partners, including the websites and apps that use our business tools.

We collect information about the people, Pages, accounts, hashtags, and groups users are connected to and how they interact with them across our Products, such as people a user communicates with the most or groups users are part of. We also collect contact information if they choose to upload, sync, or import it from a device (such as an address book or call log or SMS log history), which we use for things like helping them and others find people they may know.

The data we use to show ads to people depends on the data we have received from people. For people who are new to Facebook, we may have minimal data that we can use. For people who have used our services for longer, we likely have more data, but the amount of data will depend on the nature of that use and how they have used our controls. Any person can see each of the specific interests we maintain about them for advertising by visiting Ads Preferences, which lets people see what interests we use to choose ads for them—and to edit or delete these interests. We also provide more detailed information about how we use data to decide what ads to show to people in our "About Facebook Ads" page, at https://www.facebook.com/ads/about. And, we do not sell people's information to anyone, and we never will.

All users must expressly consent to Facebook's Terms and Data Policy when registering for Facebook. The Data Policy explains the kinds of information we collect, how we use this information, how we share this information, and how users can manage and delete information.

Facebook does not create profiles for people without a Facebook account, but we do receive some information from devices and browsers that may be used by non-users. For example:

- When people visit apps or websites that feature our technologies—like the Facebook Like or Comment button—our servers automatically log (i) standard browser or app records of the fact that a particular device or user visited the website or app (this connection to Facebook's servers occurs automatically when a person visits a website or app that contains our technologies, such as a Like button, and is an inherent function of Internet design); and (ii) any additional information the publisher of the app or website chooses to share with Facebook about the person's activities on that site (such as the fact that a purchase was made on the site). This is a standard feature of the Internet, and most websites and apps share this same information with multiple different third-parties whenever people visit their website or app. When the person visiting a website featuring Facebook's tools is not a registered Facebook user, Facebook does not have information identifying that individual, and it does not create profiles for this individual.

- We also may receive information about the device of a non-registered user if that user visits a part of Facebook that does not require people to log in—such as a public Facebook Page. The information we log when people visit our websites or apps is the same as described above and is the same information that any provider of an online service would receive.

- In addition, Facebook may receive some basic information about devices where Facebook apps are installed, including before people using those devices have registered for Facebook (such as when a user downloads a Facebook app, but has not yet created an account, or if the app is preloaded on a given device). This device data includes things like device model, operating system, IP address, app version and device identifiers. We use this information to provide the right version of the app, help people who want to create accounts (for example, optimizing the registration flow for the specific device),

retrieving bug fixes and measuring and improving app performance. We do not use this information to build profiles about non-registered users.

183. Why is it we have to pay for protection to keep our site safe?

We believe everyone deserves good privacy controls. A user owns the information they share on Facebook. This means they decide what they share and who they share it with on Facebook, and they can change their mind. We require websites and apps who use our tools to tell users they're collecting and sharing their information with us, and to get users' permission to do so.

Everyone has the right to expect strong protections for their information. We also need to do our part to help keep our community safe, in a way that's consistent with people's privacy expectations. We've recently announced several steps to give people more control over their privacy, including a new Privacy Shortcuts tool that we're rolling out now to give people information about how to control their information, including choosing who can see what they post and adding protections like two-factor authentication to their account. People can learn more about how to protect their privacy in our updated Data Policy and in our Privacy Basics feature (https://www.facebook.com/about/basics).

We are in the process of investigating every app that had access to a large amount of information before we changed our Platform in 2014. The investigation process is in full swing. We have large teams of internal and external experts working hard to investigate these apps as quickly as possible. As of early June 2018, thousands of apps have been investigated and around 200 apps have been suspended—pending a thorough investigation into whether they did in fact misuse any data. Where we find evidence that these or other apps did misuse data, we will ban them and let people know.

Facebook is generally not opposed to regulation but wants to ensure it is the right regulation. The issues facing the industry are complex, multi-faceted, and affect an important part of peoples' lives. As such, Facebook is absolutely committed to working with regulators, like Congress, to craft the right regulations. Facebook would be happy to review any proposed legislation and provide comments.

184. Do you think data and privacy issues imply that government oversight of tech companies is needed?

Protecting people's data is one of our most important responsibilities, and we are committed to continuing our work to improve how we protect people's information and to working with regulators to draft appropriate regulations. Our mission is to give people the power to build community and bring the world closer together. As the internet becomes more important in people's lives, the real question is about the right set of regulations that should apply to all internet services, regardless of size. Across the board, we have a responsibility to not just build tools, but to make sure that they're used in ways that are positive for our users. Facebook is generally not opposed to regulation but wants to ensure it is the right regulation. The issues facing the industry are complex, multi-faceted, and affect an important part of peoples' lives. As such, Facebook is absolutely committed to working with regulators, like Congress, to craft the right regulations.

We are already regulated in many ways—for example, under the Federal Trade Commission Act—and we are subject to ongoing oversight by the FTC under the terms of a 2011 consent order. We furnished extensive information to the FTC regarding the ability for users to port their Facebook data (including friends data that had been shared with them) with apps on Facebook's platform, as part of the FTC's investigation culminating in the July 27, 2012 Consent Order. The Consent Order memorializes the agreement between Facebook and the FTC and did not require Facebook to turn off or change the ability for people to port friends data that had been shared with them on Facebook to apps they used. Facebook voluntarily changed this feature of Platform in 2014, however. Facebook has not violated the Federal Trade Commission Act. Facebook is not in a position to determine whether third-party app developers violated the Act and leaves that determination to the FTC, although we can confirm that misrepresenting the terms of an app to users is a violation of Facebook's developer policies.

Facebook has inherent incentives to protect its customers' privacy and address breaches and vulnerabilities. Indeed, the recent discovery of misconduct by an app developer on the Facebook platform clearly hurt Facebook and made it harder for us to achieve our social mission. As such, Facebook is committed to protecting our platform from bad actors, ensuring we are able to continue our mission of giving people a voice and bringing them closer together. It will take some time to work through all the changes we need to make across the company, but Facebook is committed to getting this right.

185. What gives you the right to use personal information for profit and not feel responsible for knowing how it will be used?

We believe that it's important to communicate with people about the information that we collect and how people can control it. As explained in our Data Policy, we collect three basic categories of data about people:

(1) data about things people do and share (and who they connect with) on our services;

(2) data about the devices people use to access our services; and

(3) data we receive from partners, including the websites and apps that use our business tools.

We collect information about the people, Pages, accounts, hashtags, and groups users are connected to and how they interact with them across our Products, such as people a user communicates with the most or groups users are part of. We also collect contact information if they choose to upload, sync, or import it from a device (such as an address book or call log or SMS log history), which we use for things like helping them and others find people they may know.

The data we use to show ads to people depends on the data we have received from people. For people who are new to Facebook, we may have minimal data that we can use. For people who have used our services for longer, we likely have more data, but the amount of data will depend on the nature of that use and how they have used our controls. Any person can see each of the specific interests we maintain about them for advertising by visiting Ads Preferences, which lets people see what interests we use to choose ads for them—and to edit or delete these

interests. We also provide more detailed information about how we use data to decide what ads to show to people in our "About Facebook Ads" page, at https://www.facebook.com/ads/about. And, we do not sell people's information to anyone, and we never will.

All users must expressly consent to Facebook's Terms and Data Policy when registering for Facebook. The Data Policy explains the kinds of information we collect, how we use this information, how we share this information, and how users can manage and delete information.

Facebook does not create profiles for people without a Facebook account, but we do receive some information from devices and browsers that may be used by non-users. For example:

- When people visit apps or websites that feature our technologies—like the Facebook Like or Comment button—our servers automatically log (i) standard browser or app records of the fact that a particular device or user visited the website or app (this connection to Facebook's servers occurs automatically when a person visits a website or app that contains our technologies, such as a Like button, and is an inherent function of Internet design); and (ii) any additional information the publisher of the app or website chooses to share with Facebook about the person's activities on that site (such as the fact that a purchase was made on the site). This is a standard feature of the Internet, and most websites and apps share this same information with multiple different third-parties whenever people visit their website or app. When the person visiting a website featuring Facebook's tools is not a registered Facebook user, Facebook does not have information identifying that individual, and it does not create profiles for this individual.

- We also may receive information about the device of a non-registered user if that user visits a part of Facebook that does not require people to log in—such as a public Facebook Page. The information we log when people visit our websites or apps is the same as described above and is the same information that any provider of an online service would receive.

- In addition, Facebook may receive some basic information about devices where Facebook apps are installed, including before people using those devices have registered for Facebook (such as when a user downloads a Facebook app, but has not yet created an account, or if the app is preloaded on a given device). This device data includes things like device model, operating system, IP address, app version and device identifiers. We use this information to provide the right version of the app, help people who want to create accounts (for example, optimizing the registration flow for the specific device), retrieving bug fixes and measuring and improving app performance. We do not use this information to build profiles about non-registered users.

186. Should FB allow users to opt out of sharing any privacy data with ANY 3rd party users?

We believe that it's important to communicate with people about the information that we collect and how people can control it. As explained in our Data Policy, we collect three basic categories of data about people:

(1) data about things people do and share (and who they connect with) on our services;

(2) data about the devices people use to access our services; and

(3) data we receive from partners, including the websites and apps that use our business tools.

We collect information about the people, Pages, accounts, hashtags, and groups users are connected to and how they interact with them across our Products, such as people a user communicates with the most or groups users are part of. We also collect contact information if they choose to upload, sync, or import it from a device (such as an address book or call log or SMS log history), which we use for things like helping them and others find people they may know.

The data we use to show ads to people depends on the data we have received from people. For people who are new to Facebook, we may have minimal data that we can use. For people who have used our services for longer, we likely have more data, but the amount of data will depend on the nature of that use and how they have used our controls. Any person can see each of the specific interests we maintain about them for advertising by visiting Ads Preferences, which lets people see what interests we use to choose ads for them—and to edit or delete these interests. We also provide more detailed information about how we use data to decide what ads to show to people in our "About Facebook Ads" page, at https://www.facebook.com/ads/about. And, we do not sell people's information to anyone, and we never will.

All users must expressly consent to Facebook's Terms and Data Policy when registering for Facebook. The Data Policy explains the kinds of information we collect, how we use this information, how we share this information, and how users can manage and delete information.

Facebook does not create profiles for people without a Facebook account, but we do receive some information from devices and browsers that may be used by non-users. For example:

- When people visit apps or websites that feature our technologies—like the Facebook Like or Comment button—our servers automatically log (i) standard browser or app records of the fact that a particular device or user visited the website or app (this connection to Facebook's servers occurs automatically when a person visits a website or app that contains our technologies, such as a Like button, and is an inherent function of Internet design); and (ii) any additional information the publisher of the app or website chooses to share with Facebook about the person's activities on that site (such as the fact that a purchase was made on the site). This is a standard feature of the Internet, and most websites and apps share this same information with multiple different third-parties whenever people visit their website or app. When the person visiting a website featuring Facebook's tools is not a registered Facebook user, Facebook does not have information identifying that individual, and it does not create profiles for this individual.

- We also may receive information about the device of a non-registered user if that user visits a part of Facebook that does not require people to log in—such as a public

Facebook Page. The information we log when people visit our websites or apps is the same as described above and is the same information that any provider of an online service would receive.

- In addition, Facebook may receive some basic information about devices where Facebook apps are installed, including before people using those devices have registered for Facebook (such as when a user downloads a Facebook app, but has not yet created an account, or if the app is preloaded on a given device). This device data includes things like device model, operating system, IP address, app version and device identifiers. We use this information to provide the right version of the app, help people who want to create accounts (for example, optimizing the registration flow for the specific device), retrieving bug fixes and measuring and improving app performance. We do not use this information to build profiles about non-registered users.

187. When will Facebook notify users that their profiles were misappropriated?

Facebook's policies regarding third-party usage of its platform technologies have prohibited—and continue to prohibit—third-party app developers from selling or licensing user data obtained from Facebook and from sharing any user data obtained from Facebook with any ad network, data broker or other advertising or monetization-related service.

We use a variety of tools to enforce Facebook policies against violating parties, including developers. We review tens of thousands of apps per year and regularly disapprove noncompliant apps as part of our proactive review process. We also use tools like cease and desist letters, account suspensions, letter agreements, and civil litigation. For example, since 2006, Facebook has sent over 1,150 cease-and-desist letters to over 1,600 targets. In 2017, we took action against about 370,000 apps, ranging from imposing certain restrictions to removal of the app from the platform. Moreover, we have required parties who have procured our data without authorization to delete that data. We have invested significant resources in these efforts.

Recently, we announced a number of additional steps we're taking to address concerns raised by Kogan's app.

25. **Review our platform.** We will investigate all apps that had access to large amounts of data before the platform changes we announced in 2014, and we will audit any app where we identify suspicious activity. If we identify misuses of data, we'll take immediate action, including banning the app from our platform and pursuing legal action if appropriate.

26. **Tell people about data misuse.** We will tell people about apps that have misused their data. This includes building a way for people to know if their data might have been accessed via the app. Moving forward, if we remove an app, we will tell people.

27. **Turn off access for unused apps.** If someone has not used an app within the last three months, we will turn off the app's access to their data.

28. **Restrict Facebook Login data.** We are changing Login, so that the only data that an app can request without app review will include name, profile photo, and email

address. Requesting any other data will require approval from Facebook. We will also no longer allow apps to ask for access to information like religious or political views, relationship status and details, custom friends lists, education and work history, fitness activity, book reading and music listening activity, news reading, video watch activity, and games activity. We will encourage people to manage the apps they use. We already show people what apps their accounts are connected to and allow them to control what data they've permitted those apps to use. But we're making it easier for people to see what apps they use and the information they have shared with those apps.

29. **Reward people who find vulnerabilities.** We launched the Data Abuse Bounty program so that people can report to us any misuses of data by app developers.

30. **Update our policies.** We have updated our terms and Data Policy to explain how we use data and how data is shared with app developers.

188. Is Facebook willing to allow subscribers to opt out of ads and not have to pay for that?

To build a secure product with extensive infrastructure that connects people wherever they live or whatever their income level, we need to make sure everyone can afford it. Advertising lets us keep Facebook free, which ensures it remains affordable for everyone. We also believe the ads you see across the Facebook family of apps and services should be useful and relevant to you. Users can't opt out of seeing ads altogether because selling ads is what keeps Facebook free, but they do have different options to control how their data can and can't be used to show them ads. They're all found in ad preferences, which allows users to turn off the use of all data collected from partners off Facebook to target ads. Users can also decide which of their profile fields they want used for ad targeting in the Information section under "About you." Users can remove themselves from interests under "Your interests" and categories under "Your categories." And, we do not sell people's information to anyone, and we never will.

Facebook is committed to transparency for all ads, including ads with political content. Facebook believes that people should be able to easily understand why they are seeing ads, who paid for them, and what other ads those advertisers are running. As such, Facebook only allows authorized advertisers to run ads about elections or issues that are being debated across the country. In order to be authorized by Facebook, advertisers will need to confirm their identity and location. Furthermore, all political and issue ads will include a disclosure which reads: "Paid for by," and when users click on this disclosure they will be able to see details about the advertiser. Users will also be able to see an explanation of why they saw the particular ad. This is similar to the disclosure included on political TV advertisements. We just launched globally View Active Ads, a feature that will enable anyone to see all of the ads an advertiser is currently running by visiting the advertiser's Facebook Page.

189. Will you commit to not selling your customers data, and safeguarding their data?

We believe that it's important to communicate with people about the information that we collect and how people can control it. As explained in our Data Policy, we collect three basic categories of data about people:

(1) data about things people do and share (and who they connect with) on our services;

(2) data about the devices people use to access our services; and

(3) data we receive from partners, including the websites and apps that use our business tools.

We collect information about the people, Pages, accounts, hashtags, and groups users are connected to and how they interact with them across our Products, such as people a user communicates with the most or groups users are part of. We also collect contact information if they choose to upload, sync, or import it from a device (such as an address book or call log or SMS log history), which we use for things like helping them and others find people they may know.

The data we use to show ads to people depends on the data we have received from people. For people who are new to Facebook, we may have minimal data that we can use. For people who have used our services for longer, we likely have more data, but the amount of data will depend on the nature of that use and how they have used our controls. Any person can see each of the specific interests we maintain about them for advertising by visiting Ads Preferences, which lets people see what interests we use to choose ads for them—and to edit or delete these interests. We also provide more detailed information about how we use data to decide what ads to show to people in our "About Facebook Ads" page, at https://www.facebook.com/ads/about. And, we do not sell people's information to anyone, and we never will.

All users must expressly consent to Facebook's Terms and Data Policy when registering for Facebook. The Data Policy explains the kinds of information we collect, how we use this information, how we share this information, and how users can manage and delete information.

Facebook does not create profiles for people without a Facebook account, but we do receive some information from devices and browsers that may be used by non-users. For example:

- When people visit apps or websites that feature our technologies—like the Facebook Like or Comment button—our servers automatically log (i) standard browser or app records of the fact that a particular device or user visited the website or app (this connection to Facebook's servers occurs automatically when a person visits a website or app that contains our technologies, such as a Like button, and is an inherent function of Internet design); and (ii) any additional information the publisher of the app or website chooses to share with Facebook about the person's activities on that site (such as the fact that a purchase was made on the site). This is a standard feature of the Internet, and most websites and apps share this same information with multiple different third-parties whenever people visit their website or app. When the person visiting a website featuring

Facebook's tools is not a registered Facebook user, Facebook does not have information identifying that individual, and it does not create profiles for this individual.

- We also may receive information about the device of a non-registered user if that user visits a part of Facebook that does not require people to log in—such as a public Facebook Page. The information we log when people visit our websites or apps is the same as described above and is the same information that any provider of an online service would receive.

- In addition, Facebook may receive some basic information about devices where Facebook apps are installed, including before people using those devices have registered for Facebook (such as when a user downloads a Facebook app, but has not yet created an account, or if the app is preloaded on a given device). This device data includes things like device model, operating system, IP address, app version and device identifiers. We use this information to provide the right version of the app, help people who want to create accounts (for example, optimizing the registration flow for the specific device), retrieving bug fixes and measuring and improving app performance. We do not use this information to build profiles about non-registered users.

190. What guarantee do I have that friends-only data is not used outside that context?

We believe everyone deserves good privacy controls. A user owns the information they share on Facebook. This means they decide what they share and who they share it with on Facebook, and they can change their mind. We require websites and apps who use our tools to tell users they're collecting and sharing their information with us, and to get users' permission to do so.

Everyone has the right to expect strong protections for their information. We also need to do our part to help keep our community safe, in a way that's consistent with people's privacy expectations. We've recently announced several steps to give people more control over their privacy, including a new Privacy Shortcuts tool that we're rolling out now to give people information about how to control their information, including choosing who can see what they post and adding protections like two-factor authentication to their account. People can learn more about how to protect their privacy in our updated Data Policy and in our Privacy Basics feature (https://www.facebook.com/about/basics).

We are in the process of investigating every app that had access to a large amount of information before we changed our Platform in 2014. The investigation process is in full swing. We have large teams of internal and external experts working hard to investigate these apps as quickly as possible. As of early June 2018, thousands of apps have been investigated and around 200 apps have been suspended—pending a thorough investigation into whether they did in fact misuse any data. Where we find evidence that these or other apps did misuse data, we will ban them and let people know.

Facebook is generally not opposed to regulation but wants to ensure it is the right regulation. The issues facing the industry are complex, multi-faceted, and affect an important part of peoples' lives. As such, Facebook is absolutely committed to working with regulators,

like Congress, to craft the right regulations. Facebook would be happy to review any proposed legislation and provide comments.

191. How will you ensure user data privacy in future?

We believe everyone deserves good privacy controls. A user owns the information they share on Facebook. This means they decide what they share and who they share it with on Facebook, and they can change their mind. We require websites and apps who use our tools to tell users they're collecting and sharing their information with us, and to get users' permission to do so.

Everyone has the right to expect strong protections for their information. We also need to do our part to help keep our community safe, in a way that's consistent with people's privacy expectations. We've recently announced several steps to give people more control over their privacy, including a new Privacy Shortcuts tool that we're rolling out now to give people information about how to control their information, including choosing who can see what they post and adding protections like two-factor authentication to their account. People can learn more about how to protect their privacy in our updated Data Policy and in our Privacy Basics feature (https://www.facebook.com/about/basics).

We are in the process of investigating every app that had access to a large amount of information before we changed our Platform in 2014. The investigation process is in full swing. We have large teams of internal and external experts working hard to investigate these apps as quickly as possible. As of early June 2018, thousands of apps have been investigated and around 200 apps have been suspended—pending a thorough investigation into whether they did in fact misuse any data. Where we find evidence that these or other apps did misuse data, we will ban them and let people know.

Facebook is generally not opposed to regulation but wants to ensure it is the right regulation. The issues facing the industry are complex, multi-faceted, and affect an important part of peoples' lives. As such, Facebook is absolutely committed to working with regulators, like Congress, to craft the right regulations. Facebook would be happy to review any proposed legislation and provide comments.

192. How big (pervasive) do you think Facebook should be, by what measure(s)?

Protecting people's data is one of our most important responsibilities, and we are committed to continuing our work to improve how we protect people's information and to working with regulators to draft appropriate regulations. Our mission is to give people the power to build community and bring the world closer together. As the internet becomes more important in people's lives, the real question is about the right set of regulations that should apply to all internet services, regardless of size. Across the board, we have a responsibility to not just build tools, but to make sure that they're used in ways that are positive for our users. Facebook is generally not opposed to regulation but wants to ensure it is the right regulation. The issues facing the industry are complex, multi-faceted, and affect an important part of peoples' lives. As such, Facebook is absolutely committed to working with regulators, like Congress, to craft the right regulations.

We are already regulated in many ways—for example, under the Federal Trade Commission Act—and we are subject to ongoing oversight by the FTC under the terms of a 2011 consent order. We furnished extensive information to the FTC regarding the ability for users to port their Facebook data (including friends data that had been shared with them) with apps on Facebook's platform, as part of the FTC's investigation culminating in the July 27, 2012 Consent Order. The Consent Order memorializes the agreement between Facebook and the FTC and did not require Facebook to turn off or change the ability for people to port friends data that had been shared with them on Facebook to apps they used. Facebook voluntarily changed this feature of Platform in 2014, however. Facebook has not violated the Federal Trade Commission Act. Facebook is not in a position to determine whether third-party app developers violated the Act and leaves that determination to the FTC, although we can confirm that misrepresenting the terms of an app to users is a violation of Facebook's developer policies.

Facebook has inherent incentives to protect its customers' privacy and address breaches and vulnerabilities. Indeed, the recent discovery of misconduct by an app developer on the Facebook platform clearly hurt Facebook and made it harder for us to achieve our social mission. As such, Facebook is committed to protecting our platform from bad actors, ensuring we are able to continue our mission of giving people a voice and bringing them closer together. It will take some time to work through all the changes we need to make across the company, but Facebook is committed to getting this right.

193. Who were the parties involved and what data was accessed?

Facebook's policies regarding third-party usage of its platform technologies have prohibited—and continue to prohibit—third-party app developers from selling or licensing user data accessed from Facebook and from sharing any user data accessed from Facebook with any ad network, data broker or other advertising or monetization-related service. We take action on potential violations of our Platform Policies based on proactive review, external reports, and other signals. Kogan was not permitted to sell or transfer data to third-parties for the purposes he did. In doing so, Kogan and his company violated Facebook's Platform Policies.

On December 11, 2015, *The Guardian* published an article reporting that Kogan and his company, GSR, may have passed information the app had obtained from Facebook users to SCL Elections Ltd. (SCL)/Cambridge Analytica. Facebook immediately banned Kogan's app from our platform and investigated what happened and what further action Facebook should take to enforce our Platform Policies. Facebook considered the matter closed after obtaining written certifications and confirmations from Kogan, GSR, Cambridge Analytica, and SCL declaring that all such data they had obtained was accounted for and destroyed. We did not have any reason to affirmatively question the veracity of any of these certifications until March 2018, when we learned from media reporting that questions had been raised concerning the accuracy of the certifications. Facebook immediately banned Cambridge Analytica and SCL from purchasing advertisements on our services as well as removed the personal accounts of some of their officers. Moreover, while Facebook's policies in place at the time allowed us to audit apps to ensure that they were safe and did not violate its terms, we had already terminated Kogan's app's access to Facebook. Accordingly, there were no ongoing concerns about the level of data that app could access or might access in the future. With the benefit of hindsight, we wish we had

notified people whose information may have been impacted. Facebook has since notified all people potentially impacted with a detailed notice at the top of their News Feed.

194. What software or hardware systems did Facebook have to prevent hacking into accounts?

For years, we had been aware of other types of activity that appeared to come from Russian sources—largely traditional security threats such as attacking people's accounts or using social media platforms to spread stolen information. What we saw early in the 2016 campaign cycle followed this pattern. Our security team that focuses on threat intelligence—which investigates advanced security threats as part of our overall information security organization—was, from the outset, alert to the possibility of Russian activity. In several instances before November 8, 2016, this team detected and mitigated threats from actors with ties to Russia and reported them to US law enforcement officials. This included activity from a cluster of accounts we had assessed to belong to a group (APT28) that the US government has publicly linked to Russian military intelligence services. This activity, which was aimed at employees of major US political parties, fell into the normal categories of offensive cyber activities we monitor for. We warned the targets who were at highest risk, and were later in contact with law enforcement authorities about this activity.

Later in the summer we also started to see a new kind of behavior from APT28-related accounts—namely, the creation of fake personas that were then used to seed stolen information to journalists. These fake personas were organized under the banner of an organization that called itself DC Leaks. This activity violated our policies, and we removed the DC Leaks accounts.

Facebook learned from press accounts and statements by congressional leaders that Russian actors might have tried to interfere in the 2016 election by exploiting Facebook's ad tools. This is not something we had seen before, and so we started an investigation. We found that fake accounts associated with the IRA tried to influence the election.

This will never be a solved problem because we're up against determined, creative and well-funded adversaries. But we are making steady progress in preventing bad actors from using misinformation to undermine the democratic process, such as: increased ad transparency, advertiser verification and labeling, updating targeting criteria, better technological efforts to find and disable fake accounts, third-party fact checking to stop the spread of false news, doubling the number of people working on safety and security, greater industry collaboration, increased information sharing and reporting channels, proactive identification of election threats, and specific action against the Russia-based IRA.

We will continue to work with the government, and across the tech industry and civil society, to address this important national security matter so that we can do our part to prevent similar abuse from happening again.

195. Did not Facebook Users Give Permission To Share Their Data?

We believe everyone deserves good privacy controls. A user owns the information they share on Facebook. This means they decide what they share and who they share it with on

Facebook, and they can change their mind. We require websites and apps who use our tools to tell users they're collecting and sharing their information with us, and to get users' permission to do so.

Everyone has the right to expect strong protections for their information. We also need to do our part to help keep our community safe, in a way that's consistent with people's privacy expectations. We've recently announced several steps to give people more control over their privacy, including a new Privacy Shortcuts tool that we're rolling out now to give people information about how to control their information, including choosing who can see what they post and adding protections like two-factor authentication to their account. People can learn more about how to protect their privacy in our updated Data Policy and in our Privacy Basics feature (https://www.facebook.com/about/basics).

We are in the process of investigating every app that had access to a large amount of information before we changed our Platform in 2014. The investigation process is in full swing. We have large teams of internal and external experts working hard to investigate these apps as quickly as possible. As of early June 2018, thousands of apps have been investigated and around 200 apps have been suspended—pending a thorough investigation into whether they did in fact misuse any data. Where we find evidence that these or other apps did misuse data, we will ban them and let people know.

Facebook is generally not opposed to regulation but wants to ensure it is the right regulation. The issues facing the industry are complex, multi-faceted, and affect an important part of peoples' lives. As such, Facebook is absolutely committed to working with regulators, like Congress, to craft the right regulations. Facebook would be happy to review any proposed legislation and provide comments.

196. How do you use the information given you by those who sign up for FACEBOOK?

We believe that it's important to communicate with people about the information that we collect and how people can control it. As explained in our Data Policy, we collect three basic categories of data about people:

(1) data about things people do and share (and who they connect with) on our services;

(2) data about the devices people use to access our services; and

(3) data we receive from partners, including the websites and apps that use our business tools.

We collect information about the people, Pages, accounts, hashtags, and groups users are connected to and how they interact with them across our Products, such as people a user communicates with the most or groups users are part of. We also collect contact information if they choose to upload, sync, or import it from a device (such as an address book or call log or SMS log history), which we use for things like helping them and others find people they may know.

The data we use to show ads to people depends on the data we have received from people. For people who are new to Facebook, we may have minimal data that we can use. For people who have used our services for longer, we likely have more data, but the amount of data will depend on the nature of that use and how they have used our controls. Any person can see each of the specific interests we maintain about them for advertising by visiting Ads Preferences, which lets people see what interests we use to choose ads for them—and to edit or delete these interests. We also provide more detailed information about how we use data to decide what ads to show to people in our "About Facebook Ads" page, at https://www.facebook.com/ads/about. And, we do not sell people's information to anyone, and we never will.

All users must expressly consent to Facebook's Terms and Data Policy when registering for Facebook. The Data Policy explains the kinds of information we collect, how we use this information, how we share this information, and how users can manage and delete information.

Facebook does not create profiles for people without a Facebook account, but we do receive some information from devices and browsers that may be used by non-users. For example:

- When people visit apps or websites that feature our technologies—like the Facebook Like or Comment button—our servers automatically log (i) standard browser or app records of the fact that a particular device or user visited the website or app (this connection to Facebook's servers occurs automatically when a person visits a website or app that contains our technologies, such as a Like button, and is an inherent function of Internet design); and (ii) any additional information the publisher of the app or website chooses to share with Facebook about the person's activities on that site (such as the fact that a purchase was made on the site). This is a standard feature of the Internet, and most websites and apps share this same information with multiple different third-parties whenever people visit their website or app. When the person visiting a website featuring Facebook's tools is not a registered Facebook user, Facebook does not have information identifying that individual, and it does not create profiles for this individual.

- We also may receive information about the device of a non-registered user if that user visits a part of Facebook that does not require people to log in—such as a public Facebook Page. The information we log when people visit our websites or apps is the same as described above and is the same information that any provider of an online service would receive.

- In addition, Facebook may receive some basic information about devices where Facebook apps are installed, including before people using those devices have registered for Facebook (such as when a user downloads a Facebook app, but has not yet created an account, or if the app is preloaded on a given device). This device data includes things like device model, operating system, IP address, app version and device identifiers. We use this information to provide the right version of the app, help people who want to create accounts (for example, optimizing the registration flow for the specific device), retrieving bug fixes and measuring and improving app performance. We do not use this information to build profiles about non-registered users.

197. If you sincerely & primarily intended to connect friends & families, why allow the monetarization of the data to a vast array of unaccountable groups w/out promptly blocking for months after outside pressure to take action?

We believe that it's important to communicate with people about the information that we collect and how people can control it. As explained in our Data Policy, we collect three basic categories of data about people:

(1) data about things people do and share (and who they connect with) on our services;

(2) data about the devices people use to access our services; and

(3) data we receive from partners, including the websites and apps that use our business tools.

We collect information about the people, Pages, accounts, hashtags, and groups users are connected to and how they interact with them across our Products, such as people a user communicates with the most or groups users are part of. We also collect contact information if they choose to upload, sync, or import it from a device (such as an address book or call log or SMS log history), which we use for things like helping them and others find people they may know.

The data we use to show ads to people depends on the data we have received from people. For people who are new to Facebook, we may have minimal data that we can use. For people who have used our services for longer, we likely have more data, but the amount of data will depend on the nature of that use and how they have used our controls. Any person can see each of the specific interests we maintain about them for advertising by visiting Ads Preferences, which lets people see what interests we use to choose ads for them—and to edit or delete these interests. We also provide more detailed information about how we use data to decide what ads to show to people in our "About Facebook Ads" page, at https://www.facebook.com/ads/about. And, we do not sell people's information to anyone, and we never will.

All users must expressly consent to Facebook's Terms and Data Policy when registering for Facebook. The Data Policy explains the kinds of information we collect, how we use this information, how we share this information, and how users can manage and delete information.

Facebook does not create profiles for people without a Facebook account, but we do receive some information from devices and browsers that may be used by non-users. For example:

- When people visit apps or websites that feature our technologies—like the Facebook Like or Comment button—our servers automatically log (i) standard browser or app records of the fact that a particular device or user visited the website or app (this connection to Facebook's servers occurs automatically when a person visits a website or app that contains our technologies, such as a Like button, and is an inherent function of Internet design); and (ii) any additional information the publisher of the app or website chooses to share with Facebook about the person's activities on that site (such as the fact that a purchase was made on the site). This is a standard feature of the Internet, and most

websites and apps share this same information with multiple different third-parties whenever people visit their website or app. When the person visiting a website featuring Facebook's tools is not a registered Facebook user, Facebook does not have information identifying that individual, and it does not create profiles for this individual.

- We also may receive information about the device of a non-registered user if that user visits a part of Facebook that does not require people to log in—such as a public Facebook Page. The information we log when people visit our websites or apps is the same as described above and is the same information that any provider of an online service would receive.

- In addition, Facebook may receive some basic information about devices where Facebook apps are installed, including before people using those devices have registered for Facebook (such as when a user downloads a Facebook app, but has not yet created an account, or if the app is preloaded on a given device). This device data includes things like device model, operating system, IP address, app version and device identifiers. We use this information to provide the right version of the app, help people who want to create accounts (for example, optimizing the registration flow for the specific device), retrieving bug fixes and measuring and improving app performance. We do not use this information to build profiles about non-registered users.

198. If you did not use any FB apps, how much was your data exposed?

Facebook's policies regarding third-party usage of its platform technologies have prohibited—and continue to prohibit—third-party app developers from selling or licensing user data accessed from Facebook and from sharing any user data accessed from Facebook with any ad network, data broker or other advertising or monetization-related service. We take action on potential violations of our Platform Policies based on proactive review, external reports, and other signals. Kogan was not permitted to sell or transfer data to third-parties for the purposes he did. In doing so, Kogan and his company violated Facebook's Platform Policies.

On December 11, 2015, *The Guardian* published an article reporting that Kogan and his company, GSR, may have passed information the app had obtained from Facebook users to SCL Elections Ltd. (SCL)/Cambridge Analytica. Facebook immediately banned Kogan's app from our platform and investigated what happened and what further action Facebook should take to enforce our Platform Policies. Facebook considered the matter closed after obtaining written certifications and confirmations from Kogan, GSR, Cambridge Analytica, and SCL declaring that all such data they had obtained was accounted for and destroyed. We did not have any reason to affirmatively question the veracity of any of these certifications until March 2018, when we learned from media reporting that questions had been raised concerning the accuracy of the certifications. Facebook immediately banned Cambridge Analytica and SCL from purchasing advertisements on our services as well as removed the personal accounts of some of their officers. Moreover, while Facebook's policies in place at the time allowed us to audit apps to ensure that they were safe and did not violate its terms, we had already terminated Kogan's app's access to Facebook. Accordingly, there were no ongoing concerns about the level of data that app could access or might access in the future. With the benefit of hindsight, we wish we had notified people whose information may have been impacted. Facebook has since notified all people potentially impacted with a detailed notice at the top of their News Feed.

199. What other 3rd parties is this information being sold to? How will FB prevent this for ALL elections and referendums in the future?

We want our platform to be a place where people can have authentic conversations about elections and other political topics. We believe this kind of engagement promotes democracy, but we know that there are actors working to interfere with those conversations and undermine our elections. We are already taking steps to proactively prevent election interference and we are strengthening these protections going forward.

Engagement with campaigns: We want all candidates, groups, and voters to use our platform to engage in elections. We want it to be easy for people to find, follow, and contact their elected representatives—and those running to represent them. That's why, for candidates across the political spectrum, Facebook offers the same levels of support in key moments to help campaigns understand how best to use the platform. Both the Obama and Romney campaigns had access to the same tools, and no campaign received any special treatment from Facebook. Likewise, we offered identical support to both the Trump and Clinton campaigns, and had teams assigned to both. Everyone had access to the same tools, which are the same tools that every campaign is offered, and is consistent with support provided to commercial clients in the normal course of business. Facebook representatives advise political advertisers on Facebook, as they would with other, non-political managed accounts. We have a compliance team that trains our sales representatives to comply with all federal election law requirements in this area.

While no one from Facebook was assigned full-time to the Trump campaign, Facebook employees did interact with Cambridge Analytica employees. While our investigation is ongoing, our review indicates that Facebook employees did not identify any issues involving the improper use of Facebook data in the course of their interactions with Cambridge Analytica during the 2016 US Presidential campaign.

Election Integrity: In the run-up to the 2016 elections, we were focused on the kinds of cybersecurity attacks typically used by nation states, for example phishing and malware attacks. And we were too slow to spot information operations interference. Since then, we've made important changes to prevent bad actors from using misinformation to undermine the democratic process. This will never be a solved problem because we're up against determined, creative and well-funded adversaries. But we are making steady progress. Here is a list of the 10 most important changes we have made:

- **Ads transparency.** Advertising should be transparent: users should be able to see all the ads an advertiser is currently running on Facebook, Instagram and Messenger. And for ads with political content, we've created an archive that will hold ads with political content for seven years—including information about ad impressions and spend, as well as demographic data such as age, gender, and location. People in Canada and Ireland can already see all the ads that a Page is running on Facebook—and we just launched View Active Ads globally.

- **Verification and labeling.** Every advertiser will now need to confirm their ID and location before being able to run any ads with political content in the US. All ads with political content will also clearly state who paid for them.

- **Updating targeting.** We want ads on Facebook to be safe and civil. We thoroughly review the targeting criteria advertisers can use to ensure they are consistent with our principles. As a result, we removed nearly one-third of the targeting segments used by the IRA. We continue to allow some criteria that people may find controversial. But we do see businesses marketing things like historical books, documentaries or television shows using them in legitimate ways.

- **Better technology.** Over the past year, we've gotten increasingly better at finding and disabling fake accounts. We now block millions of fake accounts each day as people try to create them—and before they've done any harm. This is thanks to improvements in machine learning and artificial intelligence, which can proactively identify suspicious behavior at a scale that was not possible before—without needing to look at the content itself.

- **Action to tackle fake news.** We are working hard to stop the spread of false news. We work with third-party fact-checking organizations to limit the spread of articles rated false. To reduce the spread of false news, we remove fake accounts and disrupt economic incentives for traffickers of misinformation. We also use various signals, including feedback from our community, to identify potential false news. In countries where we have partnerships with independent third-party fact-checkers, stories rated as false by those fact-checkers are shown lower in News Feed. If Pages or domains repeatedly create or share misinformation, we significantly reduce their distribution and remove their advertising rights. We also want to empower people to decide for themselves what to read, trust, and share. We promote news literacy and work to inform people with more context. For example, if third-party fact-checkers write articles about a news story, we show them immediately below the story in the Related Articles unit. We also notify people and Page Admins if they try to share a story, or have shared one in the past, that's been determined to be false. In addition to our own efforts, we're learning from academics, scaling our partnerships with third-party fact-checkers and talking to other organizations about how we can work together.

- **Significant investments in security.** We're doubling the number of people working on safety and security from 10,000 last year to over 20,000 this year. We expect these investments to impact our profitability. But the safety of people using Facebook needs to come before profit.

- **Industry collaboration.** Recently, we joined 34 global tech and security companies in signing a TechAccord pact to help improve security for everyone.

- **Information sharing and reporting channels.** In the 2017 German elections, we worked closely with the authorities there, including the Federal Office for Information Security (BSI). This gave them a dedicated reporting channel for security issues related to the federal elections.

- **Tracking 40+ elections.** In recent months, we've started to deploy new tools and teams to proactively identify threats in the run-up to specific elections. We first

tested this effort during the Alabama Senate election, and plan to continue these efforts for elections around the globe, including the US midterms. Last year we used public service announcements to help inform people about fake news in 21 separate countries, including in advance of French, Kenyan and German elections.

- **Action against the Russia-based IRA.** In April, we removed 70 Facebook and 65 Instagram accounts—as well as 138 Facebook Pages—controlled by the IRA primarily targeted either at people living in Russia or Russian-speakers around the world including from neighboring countries like Azerbaijan, Uzbekistan, and Ukraine. The IRA has repeatedly used complex networks of inauthentic accounts to deceive and manipulate people in the US, Europe, and Russia—and we don't want them on Facebook anywhere in the world.

200. When can you provide a detailed list of everyone who has my data, data being any info with my name linked? When can you purge all my data and provide proof of the purge?

We believe that it's important to communicate with people about the information that we collect and how people can control it. As explained in our Data Policy, we collect three basic categories of data about people:

(1) data about things people do and share (and who they connect with) on our services;

(2) data about the devices people use to access our services; and

(3) data we receive from partners, including the websites and apps that use our business tools.

We collect information about the people, Pages, accounts, hashtags, and groups users are connected to and how they interact with them across our Products, such as people a user communicates with the most or groups users are part of. We also collect contact information if they choose to upload, sync, or import it from a device (such as an address book or call log or SMS log history), which we use for things like helping them and others find people they may know.

The data we use to show ads to people depends on the data we have received from people. For people who are new to Facebook, we may have minimal data that we can use. For people who have used our services for longer, we likely have more data, but the amount of data will depend on the nature of that use and how they have used our controls. Any person can see each of the specific interests we maintain about them for advertising by visiting Ads Preferences, which lets people see what interests we use to choose ads for them—and to edit or delete these interests. We also provide more detailed information about how we use data to decide what ads to show to people in our "About Facebook Ads" page, at https://www.facebook.com/ads/about. And, we do not sell people's information to anyone, and we never will.

All users must expressly consent to Facebook's Terms and Data Policy when registering for Facebook. The Data Policy explains the kinds of information we collect, how we use this information, how we share this information, and how users can manage and delete information.

Facebook does not create profiles for people without a Facebook account, but we do receive some information from devices and browsers that may be used by non-users. For example:

- When people visit apps or websites that feature our technologies—like the Facebook Like or Comment button—our servers automatically log (i) standard browser or app records of the fact that a particular device or user visited the website or app (this connection to Facebook's servers occurs automatically when a person visits a website or app that contains our technologies, such as a Like button, and is an inherent function of Internet design); and (ii) any additional information the publisher of the app or website chooses to share with Facebook about the person's activities on that site (such as the fact that a purchase was made on the site). This is a standard feature of the Internet, and most websites and apps share this same information with multiple different third-parties whenever people visit their website or app. When the person visiting a website featuring Facebook's tools is not a registered Facebook user, Facebook does not have information identifying that individual, and it does not create profiles for this individual.

- We also may receive information about the device of a non-registered user if that user visits a part of Facebook that does not require people to log in—such as a public Facebook Page. The information we log when people visit our websites or apps is the same as described above and is the same information that any provider of an online service would receive.

- In addition, Facebook may receive some basic information about devices where Facebook apps are installed, including before people using those devices have registered for Facebook (such as when a user downloads a Facebook app, but has not yet created an account, or if the app is preloaded on a given device). This device data includes things like device model, operating system, IP address, app version and device identifiers. We use this information to provide the right version of the app, help people who want to create accounts (for example, optimizing the registration flow for the specific device), retrieving bug fixes and measuring and improving app performance. We do not use this information to build profiles about non-registered users.

201. TV ads use content as target. Does FB connect people or make people TARGETS using their PII/SPI? As a parent and with my knowledge of technologies, I have raised the issue of privacy in local public schools for a long time but to no avail. I had to live with frustrations trying to raise my kids by providing an environment that allowed them to learn and grow and to make mistakes but not be defined by them or made targets. But those who made money of my children's innocence donated a fraction of it back to schools that effectively made them turn a blind eye and deaf ears to privacy concerns. The Terms of Service of Facebook and other "free" services were written to make them inculpable and they "knew" that no one would read it or understand it. The Terms of Service of Facebook and other such "free" services should be made similar to the lengthy fine-print contracts of no annual-service "free" credit cards that protects consumers. We must also be consistent in our message as leaders. If we have learned anything about the recklessness of data privacy in social networks, should leaders be encouraging

constituents to sign-up to Facebook, Twitter, or Google+ to contact them? The icons of FB, Twitter, and Google+ were there on your Contact page with no warnings to users that doing so could potentially compromise their privacy. I find such inconsistent messaging playing directly into the hands of services reaping the benefits of PII and SPI inadvertently provided by people using them. Between the phone and me, I am the smart one. Do we want to create a world where devices define who we are and trap us into stereotypes? Do we want to create a world where people can define and redefine themselves without having to also update profiles on devices around them?

We believe that it's important to communicate with people about the information that we collect and how people can control it. As explained in our Data Policy, we collect three basic categories of data about people:

(1) data about things people do and share (and who they connect with) on our services;

(2) data about the devices people use to access our services; and

(3) data we receive from partners, including the websites and apps that use our business tools.

We collect information about the people, Pages, accounts, hashtags, and groups users are connected to and how they interact with them across our Products, such as people a user communicates with the most or groups users are part of. We also collect contact information if they choose to upload, sync, or import it from a device (such as an address book or call log or SMS log history), which we use for things like helping them and others find people they may know.

The data we use to show ads to people depends on the data we have received from people. For people who are new to Facebook, we may have minimal data that we can use. For people who have used our services for longer, we likely have more data, but the amount of data will depend on the nature of that use and how they have used our controls. Any person can see each of the specific interests we maintain about them for advertising by visiting Ads Preferences, which lets people see what interests we use to choose ads for them—and to edit or delete these interests. We also provide more detailed information about how we use data to decide what ads to show to people in our "About Facebook Ads" page, at https://www.facebook.com/ads/about. And, we do not sell people's information to anyone, and we never will.

All users must expressly consent to Facebook's Terms and Data Policy when registering for Facebook. The Data Policy explains the kinds of information we collect, how we use this information, how we share this information, and how users can manage and delete information.

Facebook does not create profiles for people without a Facebook account, but we do receive some information from devices and browsers that may be used by non-users. For example:

- When people visit apps or websites that feature our technologies—like the Facebook Like or Comment button—our servers automatically log (i) standard browser or app records of

the fact that a particular device or user visited the website or app (this connection to Facebook's servers occurs automatically when a person visits a website or app that contains our technologies, such as a Like button, and is an inherent function of Internet design); and (ii) any additional information the publisher of the app or website chooses to share with Facebook about the person's activities on that site (such as the fact that a purchase was made on the site). This is a standard feature of the Internet, and most websites and apps share this same information with multiple different third-parties whenever people visit their website or app. When the person visiting a website featuring Facebook's tools is not a registered Facebook user, Facebook does not have information identifying that individual, and it does not create profiles for this individual.

- We also may receive information about the device of a non-registered user if that user visits a part of Facebook that does not require people to log in—such as a public Facebook Page. The information we log when people visit our websites or apps is the same as described above and is the same information that any provider of an online service would receive.

- In addition, Facebook may receive some basic information about devices where Facebook apps are installed, including before people using those devices have registered for Facebook (such as when a user downloads a Facebook app, but has not yet created an account, or if the app is preloaded on a given device). This device data includes things like device model, operating system, IP address, app version and device identifiers. We use this information to provide the right version of the app, help people who want to create accounts (for example, optimizing the registration flow for the specific device), retrieving bug fixes and measuring and improving app performance. We do not use this information to build profiles about non-registered users.

202. Mr. Zuckerberg, what's your plan in fighting abuse of user data?

We believe everyone deserves good privacy controls. A user owns the information they share on Facebook. This means they decide what they share and who they share it with on Facebook, and they can change their mind. We require websites and apps who use our tools to tell users they're collecting and sharing their information with us, and to get users' permission to do so.

Everyone has the right to expect strong protections for their information. We also need to do our part to help keep our community safe, in a way that's consistent with people's privacy expectations. We've recently announced several steps to give people more control over their privacy, including a new Privacy Shortcuts tool that we're rolling out now to give people information about how to control their information, including choosing who can see what they post and adding protections like two-factor authentication to their account. People can learn more about how to protect their privacy in our updated Data Policy and in our Privacy Basics feature (https://www.facebook.com/about/basics).

We are in the process of investigating every app that had access to a large amount of information before we changed our Platform in 2014. The investigation process is in full swing. We have large teams of internal and external experts working hard to investigate these apps as quickly as possible. As of early June 2018, thousands of apps have been investigated and around

200 apps have been suspended—pending a thorough investigation into whether they did in fact misuse any data. Where we find evidence that these or other apps did misuse data, we will ban them and let people know.

Facebook is generally not opposed to regulation but wants to ensure it is the right regulation. The issues facing the industry are complex, multi-faceted, and affect an important part of peoples' lives. As such, Facebook is absolutely committed to working with regulators, like Congress, to craft the right regulations. Facebook would be happy to review any proposed legislation and provide comments.

203. Is account info safe, such as private information: name, contact info if set as private

We believe everyone deserves good privacy controls. A user owns the information they share on Facebook. This means they decide what they share and who they share it with on Facebook, and they can change their mind. We require websites and apps who use our tools to tell users they're collecting and sharing their information with us, and to get users' permission to do so.

Everyone has the right to expect strong protections for their information. We also need to do our part to help keep our community safe, in a way that's consistent with people's privacy expectations. We've recently announced several steps to give people more control over their privacy, including a new Privacy Shortcuts tool that we're rolling out now to give people information about how to control their information, including choosing who can see what they post and adding protections like two-factor authentication to their account. People can learn more about how to protect their privacy in our updated Data Policy and in our Privacy Basics feature (https://www.facebook.com/about/basics).

We are in the process of investigating every app that had access to a large amount of information before we changed our Platform in 2014. The investigation process is in full swing. We have large teams of internal and external experts working hard to investigate these apps as quickly as possible. As of early June 2018, thousands of apps have been investigated and around 200 apps have been suspended—pending a thorough investigation into whether they did in fact misuse any data. Where we find evidence that these or other apps did misuse data, we will ban them and let people know.

Facebook is generally not opposed to regulation but wants to ensure it is the right regulation. The issues facing the industry are complex, multi-faceted, and affect an important part of peoples' lives. As such, Facebook is absolutely committed to working with regulators, like Congress, to craft the right regulations. Facebook would be happy to review any proposed legislation and provide comments.

204. What are you doing to PREVENT unauthorized access to users', personal data like the Cambridge Analytica breach during the 2016 Presidential election campaign?

We believe everyone deserves good privacy controls. A user owns the information they share on Facebook. This means they decide what they share and who they share it with on Facebook, and they can change their mind. We require websites and apps who use our tools to

tell users they're collecting and sharing their information with us, and to get users' permission to do so.

Everyone has the right to expect strong protections for their information. We also need to do our part to help keep our community safe, in a way that's consistent with people's privacy expectations. We've recently announced several steps to give people more control over their privacy, including a new Privacy Shortcuts tool that we're rolling out now to give people information about how to control their information, including choosing who can see what they post and adding protections like two-factor authentication to their account. People can learn more about how to protect their privacy in our updated Data Policy and in our Privacy Basics feature (https://www.facebook.com/about/basics).

We are in the process of investigating every app that had access to a large amount of information before we changed our Platform in 2014. The investigation process is in full swing. We have large teams of internal and external experts working hard to investigate these apps as quickly as possible. As of early June 2018, thousands of apps have been investigated and around 200 apps have been suspended—pending a thorough investigation into whether they did in fact misuse any data. Where we find evidence that these or other apps did misuse data, we will ban them and let people know.

Facebook is generally not opposed to regulation but wants to ensure it is the right regulation. The issues facing the industry are complex, multi-faceted, and affect an important part of peoples' lives. As such, Facebook is absolutely committed to working with regulators, like Congress, to craft the right regulations. Facebook would be happy to review any proposed legislation and provide comments.

205. What will Facebook do to protect users?

We believe everyone deserves good privacy controls. A user owns the information they share on Facebook. This means they decide what they share and who they share it with on Facebook, and they can change their mind. We require websites and apps who use our tools to tell users they're collecting and sharing their information with us, and to get users' permission to do so.

Everyone has the right to expect strong protections for their information. We also need to do our part to help keep our community safe, in a way that's consistent with people's privacy expectations. We've recently announced several steps to give people more control over their privacy, including a new Privacy Shortcuts tool that we're rolling out now to give people information about how to control their information, including choosing who can see what they post and adding protections like two-factor authentication to their account. People can learn more about how to protect their privacy in our updated Data Policy and in our Privacy Basics feature (https://www.facebook.com/about/basics).

We are in the process of investigating every app that had access to a large amount of information before we changed our Platform in 2014. The investigation process is in full swing. We have large teams of internal and external experts working hard to investigate these apps as quickly as possible. As of early June 2018, thousands of apps have been investigated and around

200 apps have been suspended—pending a thorough investigation into whether they did in fact misuse any data. Where we find evidence that these or other apps did misuse data, we will ban them and let people know.

Facebook is generally not opposed to regulation but wants to ensure it is the right regulation. The issues facing the industry are complex, multi-faceted, and affect an important part of peoples' lives. As such, Facebook is absolutely committed to working with regulators, like Congress, to craft the right regulations. Facebook would be happy to review any proposed legislation and provide comments.

206. I think that the basic question is:

"What is the potential impact of having this data stolen?
The answer should include implications on their (those affected) personal, financial and social their effects."

2nd question is:

"What safeguards will be implemented to prevent data breeches in the future."

3rd supplemental question is:

"What methods of assuring privacy will be implemented in their processes"

We believe everyone deserves good privacy controls. A user owns the information they share on Facebook. This means they decide what they share and who they share it with on Facebook, and they can change their mind. We require websites and apps who use our tools to tell users they're collecting and sharing their information with us, and to get users' permission to do so.

Everyone has the right to expect strong protections for their information. We also need to do our part to help keep our community safe, in a way that's consistent with people's privacy expectations. We've recently announced several steps to give people more control over their privacy, including a new Privacy Shortcuts tool that we're rolling out now to give people information about how to control their information, including choosing who can see what they post and adding protections like two-factor authentication to their account. People can learn more about how to protect their privacy in our updated Data Policy and in our Privacy Basics feature (https://www.facebook.com/about/basics).

We are in the process of investigating every app that had access to a large amount of information before we changed our Platform in 2014. The investigation process is in full swing. We have large teams of internal and external experts working hard to investigate these apps as quickly as possible. As of early June 2018, thousands of apps have been investigated and around 200 apps have been suspended—pending a thorough investigation into whether they did in fact misuse any data. Where we find evidence that these or other apps did misuse data, we will ban them and let people know.

Facebook is generally not opposed to regulation but wants to ensure it is the right regulation. The issues facing the industry are complex, multi-faceted, and affect an important part of peoples' lives. As such, Facebook is absolutely committed to working with regulators, like Congress, to craft the right regulations. Facebook would be happy to review any proposed legislation and provide comments.

207. Can he ensure only anonymous data is shared?

We believe that it's important to communicate with people about the information that we collect and how people can control it. As explained in our Data Policy, we collect three basic categories of data about people:

(1) data about things people do and share (and who they connect with) on our services;

(2) data about the devices people use to access our services; and

(3) data we receive from partners, including the websites and apps that use our business tools.

We collect information about the people, Pages, accounts, hashtags, and groups users are connected to and how they interact with them across our Products, such as people a user communicates with the most or groups users are part of. We also collect contact information if they choose to upload, sync, or import it from a device (such as an address book or call log or SMS log history), which we use for things like helping them and others find people they may know.

The data we use to show ads to people depends on the data we have received from people. For people who are new to Facebook, we may have minimal data that we can use. For people who have used our services for longer, we likely have more data, but the amount of data will depend on the nature of that use and how they have used our controls. Any person can see each of the specific interests we maintain about them for advertising by visiting Ads Preferences, which lets people see what interests we use to choose ads for them—and to edit or delete these interests. We also provide more detailed information about how we use data to decide what ads to show to people in our "About Facebook Ads" page, at https://www.facebook.com/ads/about. And, we do not sell people's information to anyone, and we never will.

All users must expressly consent to Facebook's Terms and Data Policy when registering for Facebook. The Data Policy explains the kinds of information we collect, how we use this information, how we share this information, and how users can manage and delete information.

Facebook does not create profiles for people without a Facebook account, but we do receive some information from devices and browsers that may be used by non-users. For example:

- When people visit apps or websites that feature our technologies—like the Facebook Like or Comment button—our servers automatically log (i) standard browser or app records of the fact that a particular device or user visited the website or app (this connection to Facebook's servers occurs automatically when a person visits a website or app that

contains our technologies, such as a Like button, and is an inherent function of Internet design); and (ii) any additional information the publisher of the app or website chooses to share with Facebook about the person's activities on that site (such as the fact that a purchase was made on the site). This is a standard feature of the Internet, and most websites and apps share this same information with multiple different third-parties whenever people visit their website or app. When the person visiting a website featuring Facebook's tools is not a registered Facebook user, Facebook does not have information identifying that individual, and it does not create profiles for this individual.

- We also may receive information about the device of a non-registered user if that user visits a part of Facebook that does not require people to log in—such as a public Facebook Page. The information we log when people visit our websites or apps is the same as described above and is the same information that any provider of an online service would receive.

- In addition, Facebook may receive some basic information about devices where Facebook apps are installed, including before people using those devices have registered for Facebook (such as when a user downloads a Facebook app, but has not yet created an account, or if the app is preloaded on a given device). This device data includes things like device model, operating system, IP address, app version and device identifiers. We use this information to provide the right version of the app, help people who want to create accounts (for example, optimizing the registration flow for the specific device), retrieving bug fixes and measuring and improving app performance. We do not use this information to build profiles about non-registered users.

208. Does FB really delete personal info when users request so? Are FB aware others accessing their data? If so, what they do? If not, why not?

We believe that it's important to communicate with people about the information that we collect and how people can control it. As explained in our Data Policy, we collect three basic categories of data about people:

(1) data about things people do and share (and who they connect with) on our services;

(2) data about the devices people use to access our services; and

(3) data we receive from partners, including the websites and apps that use our business tools.

We collect information about the people, Pages, accounts, hashtags, and groups users are connected to and how they interact with them across our Products, such as people a user communicates with the most or groups users are part of. We also collect contact information if they choose to upload, sync, or import it from a device (such as an address book or call log or SMS log history), which we use for things like helping them and others find people they may know.

The data we use to show ads to people depends on the data we have received from people. For people who are new to Facebook, we may have minimal data that we can use. For

people who have used our services for longer, we likely have more data, but the amount of data will depend on the nature of that use and how they have used our controls. Any person can see each of the specific interests we maintain about them for advertising by visiting Ads Preferences, which lets people see what interests we use to choose ads for them—and to edit or delete these interests. We also provide more detailed information about how we use data to decide what ads to show to people in our "About Facebook Ads" page, at https://www.facebook.com/ads/about. And, we do not sell people's information to anyone, and we never will.

All users must expressly consent to Facebook's Terms and Data Policy when registering for Facebook. The Data Policy explains the kinds of information we collect, how we use this information, how we share this information, and how users can manage and delete information.

Facebook does not create profiles for people without a Facebook account, but we do receive some information from devices and browsers that may be used by non-users. For example:

- When people visit apps or websites that feature our technologies—like the Facebook Like or Comment button—our servers automatically log (i) standard browser or app records of the fact that a particular device or user visited the website or app (this connection to Facebook's servers occurs automatically when a person visits a website or app that contains our technologies, such as a Like button, and is an inherent function of Internet design); and (ii) any additional information the publisher of the app or website chooses to share with Facebook about the person's activities on that site (such as the fact that a purchase was made on the site). This is a standard feature of the Internet, and most websites and apps share this same information with multiple different third-parties whenever people visit their website or app. When the person visiting a website featuring Facebook's tools is not a registered Facebook user, Facebook does not have information identifying that individual, and it does not create profiles for this individual.

- We also may receive information about the device of a non-registered user if that user visits a part of Facebook that does not require people to log in—such as a public Facebook Page. The information we log when people visit our websites or apps is the same as described above and is the same information that any provider of an online service would receive.

- In addition, Facebook may receive some basic information about devices where Facebook apps are installed, including before people using those devices have registered for Facebook (such as when a user downloads a Facebook app, but has not yet created an account, or if the app is preloaded on a given device). This device data includes things like device model, operating system, IP address, app version and device identifiers. We use this information to provide the right version of the app, help people who want to create accounts (for example, optimizing the registration flow for the specific device), retrieving bug fixes and measuring and improving app performance. We do not use this information to build profiles about non-registered users.

209. To protect user privacy, is user data anonymized before being shared outside Facebook?

We believe that it's important to communicate with people about the information that we collect and how people can control it. As explained in our Data Policy, we collect three basic categories of data about people:

(1) data about things people do and share (and who they connect with) on our services;

(2) data about the devices people use to access our services; and

(3) data we receive from partners, including the websites and apps that use our business tools.

We collect information about the people, Pages, accounts, hashtags, and groups users are connected to and how they interact with them across our Products, such as people a user communicates with the most or groups users are part of. We also collect contact information if they choose to upload, sync, or import it from a device (such as an address book or call log or SMS log history), which we use for things like helping them and others find people they may know.

The data we use to show ads to people depends on the data we have received from people. For people who are new to Facebook, we may have minimal data that we can use. For people who have used our services for longer, we likely have more data, but the amount of data will depend on the nature of that use and how they have used our controls. Any person can see each of the specific interests we maintain about them for advertising by visiting Ads Preferences, which lets people see what interests we use to choose ads for them—and to edit or delete these interests. We also provide more detailed information about how we use data to decide what ads to show to people in our "About Facebook Ads" page, at https://www.facebook.com/ads/about. And, we do not sell people's information to anyone, and we never will.

All users must expressly consent to Facebook's Terms and Data Policy when registering for Facebook. The Data Policy explains the kinds of information we collect, how we use this information, how we share this information, and how users can manage and delete information.

Facebook does not create profiles for people without a Facebook account, but we do receive some information from devices and browsers that may be used by non-users. For example:

- When people visit apps or websites that feature our technologies—like the Facebook Like or Comment button—our servers automatically log (i) standard browser or app records of the fact that a particular device or user visited the website or app (this connection to Facebook's servers occurs automatically when a person visits a website or app that contains our technologies, such as a Like button, and is an inherent function of Internet design); and (ii) any additional information the publisher of the app or website chooses to share with Facebook about the person's activities on that site (such as the fact that a purchase was made on the site). This is a standard feature of the Internet, and most websites and apps share this same information with multiple different third-parties whenever people visit their website or app. When the person visiting a website featuring

Facebook's tools is not a registered Facebook user, Facebook does not have information identifying that individual, and it does not create profiles for this individual.

- We also may receive information about the device of a non-registered user if that user visits a part of Facebook that does not require people to log in—such as a public Facebook Page. The information we log when people visit our websites or apps is the same as described above and is the same information that any provider of an online service would receive.

- In addition, Facebook may receive some basic information about devices where Facebook apps are installed, including before people using those devices have registered for Facebook (such as when a user downloads a Facebook app, but has not yet created an account, or if the app is preloaded on a given device). This device data includes things like device model, operating system, IP address, app version and device identifiers. We use this information to provide the right version of the app, help people who want to create accounts (for example, optimizing the registration flow for the specific device), retrieving bug fixes and measuring and improving app performance. We do not use this information to build profiles about non-registered users.

210. How are users to trust whatever FB puts into place, isn't it too little too late?

We believe everyone deserves good privacy controls. A user owns the information they share on Facebook. This means they decide what they share and who they share it with on Facebook, and they can change their mind. We require websites and apps who use our tools to tell users they're collecting and sharing their information with us, and to get users' permission to do so.

Everyone has the right to expect strong protections for their information. We also need to do our part to help keep our community safe, in a way that's consistent with people's privacy expectations. We've recently announced several steps to give people more control over their privacy, including a new Privacy Shortcuts tool that we're rolling out now to give people information about how to control their information, including choosing who can see what they post and adding protections like two-factor authentication to their account. People can learn more about how to protect their privacy in our updated Data Policy and in our Privacy Basics feature (https://www.facebook.com/about/basics).

We are in the process of investigating every app that had access to a large amount of information before we changed our Platform in 2014. The investigation process is in full swing. We have large teams of internal and external experts working hard to investigate these apps as quickly as possible. As of early June 2018, thousands of apps have been investigated and around 200 apps have been suspended—pending a thorough investigation into whether they did in fact misuse any data. Where we find evidence that these or other apps did misuse data, we will ban them and let people know.

Facebook is generally not opposed to regulation but wants to ensure it is the right regulation. The issues facing the industry are complex, multi-faceted, and affect an important part of peoples' lives. As such, Facebook is absolutely committed to working with regulators,

like Congress, to craft the right regulations. Facebook would be happy to review any proposed legislation and provide comments.

211. Will you promise that people who quit FB will have all their data deleted?

We believe everyone deserves good privacy controls. A user owns the information they share on Facebook. This means they decide what they share and who they share it with on Facebook, and they can change their mind. We require websites and apps who use our tools to tell users they're collecting and sharing their information with us, and to get users' permission to do so.

Everyone has the right to expect strong protections for their information. We also need to do our part to help keep our community safe, in a way that's consistent with people's privacy expectations. We've recently announced several steps to give people more control over their privacy, including a new Privacy Shortcuts tool that we're rolling out now to give people information about how to control their information, including choosing who can see what they post and adding protections like two-factor authentication to their account. People can learn more about how to protect their privacy in our updated Data Policy and in our Privacy Basics feature (https://www.facebook.com/about/basics).

We are in the process of investigating every app that had access to a large amount of information before we changed our Platform in 2014. The investigation process is in full swing. We have large teams of internal and external experts working hard to investigate these apps as quickly as possible. As of early June 2018, thousands of apps have been investigated and around 200 apps have been suspended—pending a thorough investigation into whether they did in fact misuse any data. Where we find evidence that these or other apps did misuse data, we will ban them and let people know.

Facebook is generally not opposed to regulation but wants to ensure it is the right regulation. The issues facing the industry are complex, multi-faceted, and affect an important part of peoples' lives. As such, Facebook is absolutely committed to working with regulators, like Congress, to craft the right regulations. Facebook would be happy to review any proposed legislation and provide comments.

212. Is there any reason we should trust Facebook with our privacy data? What safeguards are in place to?

We believe everyone deserves good privacy controls. A user owns the information they share on Facebook. This means they decide what they share and who they share it with on Facebook, and they can change their mind. We require websites and apps who use our tools to tell users they're collecting and sharing their information with us, and to get users' permission to do so.

Everyone has the right to expect strong protections for their information. We also need to do our part to help keep our community safe, in a way that's consistent with people's privacy expectations. We've recently announced several steps to give people more control over their privacy, including a new Privacy Shortcuts tool that we're rolling out now to give people information about how to control their information, including choosing who can see what they

post and adding protections like two-factor authentication to their account. People can learn more about how to protect their privacy in our updated Data Policy and in our Privacy Basics feature (https://www.facebook.com/about/basics).

We are in the process of investigating every app that had access to a large amount of information before we changed our Platform in 2014. The investigation process is in full swing. We have large teams of internal and external experts working hard to investigate these apps as quickly as possible. As of early June 2018, thousands of apps have been investigated and around 200 apps have been suspended—pending a thorough investigation into whether they did in fact misuse any data. Where we find evidence that these or other apps did misuse data, we will ban them and let people know.

Facebook is generally not opposed to regulation but wants to ensure it is the right regulation. The issues facing the industry are complex, multi-faceted, and affect an important part of peoples' lives. As such, Facebook is absolutely committed to working with regulators, like Congress, to craft the right regulations. Facebook would be happy to review any proposed legislation and provide comments.

213. Why would Facebook think it was OK for a user's friend to be able to give away that user's personal data to unknown 3rd parties?

We believe everyone deserves good privacy controls. A user owns the information they share on Facebook. This means they decide what they share and who they share it with on Facebook, and they can change their mind. We require websites and apps who use our tools to tell users they're collecting and sharing their information with us, and to get users' permission to do so.

Everyone has the right to expect strong protections for their information. We also need to do our part to help keep our community safe, in a way that's consistent with people's privacy expectations. We've recently announced several steps to give people more control over their privacy, including a new Privacy Shortcuts tool that we're rolling out now to give people information about how to control their information, including choosing who can see what they post and adding protections like two-factor authentication to their account. People can learn more about how to protect their privacy in our updated Data Policy and in our Privacy Basics feature (https://www.facebook.com/about/basics).

We are in the process of investigating every app that had access to a large amount of information before we changed our Platform in 2014. The investigation process is in full swing. We have large teams of internal and external experts working hard to investigate these apps as quickly as possible. As of early June 2018, thousands of apps have been investigated and around 200 apps have been suspended—pending a thorough investigation into whether they did in fact misuse any data. Where we find evidence that these or other apps did misuse data, we will ban them and let people know.

Facebook is generally not opposed to regulation but wants to ensure it is the right regulation. The issues facing the industry are complex, multi-faceted, and affect an important part of peoples' lives. As such, Facebook is absolutely committed to working with regulators,

like Congress, to craft the right regulations. Facebook would be happy to review any proposed legislation and provide comments.

214. Can anyone buy access? Do you have any criteria?

We believe that it's important to communicate with people about the information that we collect and how people can control it. As explained in our Data Policy, we collect three basic categories of data about people:

(1) data about things people do and share (and who they connect with) on our services;

(2) data about the devices people use to access our services; and

(3) data we receive from partners, including the websites and apps that use our business tools.

We collect information about the people, Pages, accounts, hashtags, and groups users are connected to and how they interact with them across our Products, such as people a user communicates with the most or groups users are part of. We also collect contact information if they choose to upload, sync, or import it from a device (such as an address book or call log or SMS log history), which we use for things like helping them and others find people they may know.

The data we use to show ads to people depends on the data we have received from people. For people who are new to Facebook, we may have minimal data that we can use. For people who have used our services for longer, we likely have more data, but the amount of data will depend on the nature of that use and how they have used our controls. Any person can see each of the specific interests we maintain about them for advertising by visiting Ads Preferences, which lets people see what interests we use to choose ads for them—and to edit or delete these interests. We also provide more detailed information about how we use data to decide what ads to show to people in our "About Facebook Ads" page, at https://www.facebook.com/ads/about. And, we do not sell people's information to anyone, and we never will.

All users must expressly consent to Facebook's Terms and Data Policy when registering for Facebook. The Data Policy explains the kinds of information we collect, how we use this information, how we share this information, and how users can manage and delete information.

Facebook does not create profiles for people without a Facebook account, but we do receive some information from devices and browsers that may be used by non-users. For example:

- When people visit apps or websites that feature our technologies—like the Facebook Like or Comment button—our servers automatically log (i) standard browser or app records of the fact that a particular device or user visited the website or app (this connection to Facebook's servers occurs automatically when a person visits a website or app that contains our technologies, such as a Like button, and is an inherent function of Internet design); and (ii) any additional information the publisher of the app or website chooses to share with Facebook about the person's activities on that site (such as the fact that a

purchase was made on the site). This is a standard feature of the Internet, and most websites and apps share this same information with multiple different third-parties whenever people visit their website or app. When the person visiting a website featuring Facebook's tools is not a registered Facebook user, Facebook does not have information identifying that individual, and it does not create profiles for this individual.

- We also may receive information about the device of a non-registered user if that user visits a part of Facebook that does not require people to log in—such as a public Facebook Page. The information we log when people visit our websites or apps is the same as described above and is the same information that any provider of an online service would receive.

- In addition, Facebook may receive some basic information about devices where Facebook apps are installed, including before people using those devices have registered for Facebook (such as when a user downloads a Facebook app, but has not yet created an account, or if the app is preloaded on a given device). This device data includes things like device model, operating system, IP address, app version and device identifiers. We use this information to provide the right version of the app, help people who want to create accounts (for example, optimizing the registration flow for the specific device), retrieving bug fixes and measuring and improving app performance. We do not use this information to build profiles about non-registered users.

215. Does Facebook have any constraints /guards in place to protect users' personal data or have they always been selling it? If we have an account, should we assume that dell our privacy has been breached?

We believe that it's important to communicate with people about the information that we collect and how people can control it. As explained in our Data Policy, we collect three basic categories of data about people:

(1) data about things people do and share (and who they connect with) on our services;

(2) data about the devices people use to access our services; and

(3) data we receive from partners, including the websites and apps that use our business tools.

We collect information about the people, Pages, accounts, hashtags, and groups users are connected to and how they interact with them across our Products, such as people a user communicates with the most or groups users are part of. We also collect contact information if they choose to upload, sync, or import it from a device (such as an address book or call log or SMS log history), which we use for things like helping them and others find people they may know.

The data we use to show ads to people depends on the data we have received from people. For people who are new to Facebook, we may have minimal data that we can use. For people who have used our services for longer, we likely have more data, but the amount of data will depend on the nature of that use and how they have used our controls. Any person can see

each of the specific interests we maintain about them for advertising by visiting Ads Preferences, which lets people see what interests we use to choose ads for them—and to edit or delete these interests. We also provide more detailed information about how we use data to decide what ads to show to people in our "About Facebook Ads" page, at https://www.facebook.com/ads/about. And, we do not sell people's information to anyone, and we never will.

All users must expressly consent to Facebook's Terms and Data Policy when registering for Facebook. The Data Policy explains the kinds of information we collect, how we use this information, how we share this information, and how users can manage and delete information.

Facebook does not create profiles for people without a Facebook account, but we do receive some information from devices and browsers that may be used by non-users. For example:

- When people visit apps or websites that feature our technologies—like the Facebook Like or Comment button—our servers automatically log (i) standard browser or app records of the fact that a particular device or user visited the website or app (this connection to Facebook's servers occurs automatically when a person visits a website or app that contains our technologies, such as a Like button, and is an inherent function of Internet design); and (ii) any additional information the publisher of the app or website chooses to share with Facebook about the person's activities on that site (such as the fact that a purchase was made on the site). This is a standard feature of the Internet, and most websites and apps share this same information with multiple different third-parties whenever people visit their website or app. When the person visiting a website featuring Facebook's tools is not a registered Facebook user, Facebook does not have information identifying that individual, and it does not create profiles for this individual.

- We also may receive information about the device of a non-registered user if that user visits a part of Facebook that does not require people to log in—such as a public Facebook Page. The information we log when people visit our websites or apps is the same as described above and is the same information that any provider of an online service would receive.

- In addition, Facebook may receive some basic information about devices where Facebook apps are installed, including before people using those devices have registered for Facebook (such as when a user downloads a Facebook app, but has not yet created an account, or if the app is preloaded on a given device). This device data includes things like device model, operating system, IP address, app version and device identifiers. We use this information to provide the right version of the app, help people who want to create accounts (for example, optimizing the registration flow for the specific device), retrieving bug fixes and measuring and improving app performance. We do not use this information to build profiles about non-registered users.

216. Is money more important than privacy?

We believe everyone deserves good privacy controls. A user owns the information they share on Facebook. This means they decide what they share and who they share it with on Facebook, and they can change their mind. We require websites and apps who use our tools to

tell users they're collecting and sharing their information with us, and to get users' permission to do so.

Everyone has the right to expect strong protections for their information. We also need to do our part to help keep our community safe, in a way that's consistent with people's privacy expectations. We've recently announced several steps to give people more control over their privacy, including a new Privacy Shortcuts tool that we're rolling out now to give people information about how to control their information, including choosing who can see what they post and adding protections like two-factor authentication to their account. People can learn more about how to protect their privacy in our updated Data Policy and in our Privacy Basics feature (https://www.facebook.com/about/basics).

We are in the process of investigating every app that had access to a large amount of information before we changed our Platform in 2014. The investigation process is in full swing. We have large teams of internal and external experts working hard to investigate these apps as quickly as possible. As of early June 2018, thousands of apps have been investigated and around 200 apps have been suspended—pending a thorough investigation into whether they did in fact misuse any data. Where we find evidence that these or other apps did misuse data, we will ban them and let people know.

Facebook is generally not opposed to regulation but wants to ensure it is the right regulation. The issues facing the industry are complex, multi-faceted, and affect an important part of peoples' lives. As such, Facebook is absolutely committed to working with regulators, like Congress, to craft the right regulations. Facebook would be happy to review any proposed legislation and provide comments.

217. When did you really know that Cambridge Analytica misused data?

Facebook's policies regarding third-party usage of its platform technologies have prohibited—and continue to prohibit—third-party app developers from selling or licensing user data accessed from Facebook and from sharing any user data accessed from Facebook with any ad network, data broker or other advertising or monetization-related service. We take action on potential violations of our Platform Policies based on proactive review, external reports, and other signals. Kogan was not permitted to sell or transfer data to third-parties for the purposes he did. In doing so, Kogan and his company violated Facebook's Platform Policies.

On December 11, 2015, *The Guardian* published an article reporting that Kogan and his company, GSR, may have passed information the app had obtained from Facebook users to SCL Elections Ltd. (SCL)/Cambridge Analytica. Facebook immediately banned Kogan's app from our platform and investigated what happened and what further action Facebook should take to enforce our Platform Policies. Facebook considered the matter closed after obtaining written certifications and confirmations from Kogan, GSR, Cambridge Analytica, and SCL declaring that all such data they had obtained was accounted for and destroyed. We did not have any reason to affirmatively question the veracity of any of these certifications until March 2018, when we learned from media reporting that questions had been raised concerning the accuracy of the certifications. Facebook immediately banned Cambridge Analytica and SCL from purchasing advertisements on our services as well as removed the personal accounts of some of their

officers. Moreover, while Facebook's policies in place at the time allowed us to audit apps to ensure that they were safe and did not violate its terms, we had already terminated Kogan's app's access to Facebook. Accordingly, there were no ongoing concerns about the level of data that app could access or might access in the future. With the benefit of hindsight, we wish we had notified people whose information may have been impacted. Facebook has since notified all people potentially impacted with a detailed notice at the top of their News Feed.

218. When did FBook 1st allow 3rd party access and did you receive any remuneration for it?

We believe that it's important to communicate with people about the information that we collect and how people can control it. As explained in our Data Policy, we collect three basic categories of data about people:

(1) data about things people do and share (and who they connect with) on our services;

(2) data about the devices people use to access our services; and

(3) data we receive from partners, including the websites and apps that use our business tools.

We collect information about the people, Pages, accounts, hashtags, and groups users are connected to and how they interact with them across our Products, such as people a user communicates with the most or groups users are part of. We also collect contact information if they choose to upload, sync, or import it from a device (such as an address book or call log or SMS log history), which we use for things like helping them and others find people they may know.

The data we use to show ads to people depends on the data we have received from people. For people who are new to Facebook, we may have minimal data that we can use. For people who have used our services for longer, we likely have more data, but the amount of data will depend on the nature of that use and how they have used our controls. Any person can see each of the specific interests we maintain about them for advertising by visiting Ads Preferences, which lets people see what interests we use to choose ads for them—and to edit or delete these interests. We also provide more detailed information about how we use data to decide what ads to show to people in our "About Facebook Ads" page, at https://www.facebook.com/ads/about. And, we do not sell people's information to anyone, and we never will.

All users must expressly consent to Facebook's Terms and Data Policy when registering for Facebook. The Data Policy explains the kinds of information we collect, how we use this information, how we share this information, and how users can manage and delete information.

Facebook does not create profiles for people without a Facebook account, but we do receive some information from devices and browsers that may be used by non-users. For example:

- When people visit apps or websites that feature our technologies—like the Facebook Like or Comment button—our servers automatically log (i) standard browser or app records of

the fact that a particular device or user visited the website or app (this connection to Facebook's servers occurs automatically when a person visits a website or app that contains our technologies, such as a Like button, and is an inherent function of Internet design); and (ii) any additional information the publisher of the app or website chooses to share with Facebook about the person's activities on that site (such as the fact that a purchase was made on the site). This is a standard feature of the Internet, and most websites and apps share this same information with multiple different third-parties whenever people visit their website or app. When the person visiting a website featuring Facebook's tools is not a registered Facebook user, Facebook does not have information identifying that individual, and it does not create profiles for this individual.

- We also may receive information about the device of a non-registered user if that user visits a part of Facebook that does not require people to log in—such as a public Facebook Page. The information we log when people visit our websites or apps is the same as described above and is the same information that any provider of an online service would receive.

- In addition, Facebook may receive some basic information about devices where Facebook apps are installed, including before people using those devices have registered for Facebook (such as when a user downloads a Facebook app, but has not yet created an account, or if the app is preloaded on a given device). This device data includes things like device model, operating system, IP address, app version and device identifiers. We use this information to provide the right version of the app, help people who want to create accounts (for example, optimizing the registration flow for the specific device), retrieving bug fixes and measuring and improving app performance. We do not use this information to build profiles about non-registered users.

219. How is it that you didn't anticipate this?

Facebook's policies regarding third-party usage of its platform technologies have prohibited—and continue to prohibit—third-party app developers from selling or licensing user data accessed from Facebook and from sharing any user data accessed from Facebook with any ad network, data broker or other advertising or monetization-related service. We take action on potential violations of our Platform Policies based on proactive review, external reports, and other signals. Kogan was not permitted to sell or transfer data to third-parties for the purposes he did. In doing so, Kogan and his company violated Facebook's Platform Policies.

On December 11, 2015, *The Guardian* published an article reporting that Kogan and his company, GSR, may have passed information the app had obtained from Facebook users to SCL Elections Ltd. (SCL)/Cambridge Analytica. Facebook immediately banned Kogan's app from our platform and investigated what happened and what further action Facebook should take to enforce our Platform Policies. Facebook considered the matter closed after obtaining written certifications and confirmations from Kogan, GSR, Cambridge Analytica, and SCL declaring that all such data they had obtained was accounted for and destroyed. We did not have any reason to affirmatively question the veracity of any of these certifications until March 2018, when we learned from media reporting that questions had been raised concerning the accuracy of the certifications. Facebook immediately banned Cambridge Analytica and SCL from purchasing

advertisements on our services as well as removed the personal accounts of some of their officers. Moreover, while Facebook's policies in place at the time allowed us to audit apps to ensure that they were safe and did not violate its terms, we had already terminated Kogan's app's access to Facebook. Accordingly, there were no ongoing concerns about the level of data that app could access or might access in the future. With the benefit of hindsight, we wish we had notified people whose information may have been impacted. Facebook has since notified all people potentially impacted with a detailed notice at the top of their News Feed.

220. Did you know, and how do we know this won't occur again?

Facebook's policies regarding third-party usage of its platform technologies have prohibited—and continue to prohibit—third-party app developers from selling or licensing user data accessed from Facebook and from sharing any user data accessed from Facebook with any ad network, data broker or other advertising or monetization-related service. We take action on potential violations of our Platform Policies based on proactive review, external reports, and other signals. Kogan was not permitted to sell or transfer data to third-parties for the purposes he did. In doing so, Kogan and his company violated Facebook's Platform Policies.

On December 11, 2015, *The Guardian* published an article reporting that Kogan and his company, GSR, may have passed information the app had obtained from Facebook users to SCL Elections Ltd. (SCL)/Cambridge Analytica. Facebook immediately banned Kogan's app from our platform and investigated what happened and what further action Facebook should take to enforce our Platform Policies. Facebook considered the matter closed after obtaining written certifications and confirmations from Kogan, GSR, Cambridge Analytica, and SCL declaring that all such data they had obtained was accounted for and destroyed. We did not have any reason to affirmatively question the veracity of any of these certifications until March 2018, when we learned from media reporting that questions had been raised concerning the accuracy of the certifications. Facebook immediately banned Cambridge Analytica and SCL from purchasing advertisements on our services as well as removed the personal accounts of some of their officers. Moreover, while Facebook's policies in place at the time allowed us to audit apps to ensure that they were safe and did not violate its terms, we had already terminated Kogan's app's access to Facebook. Accordingly, there were no ongoing concerns about the level of data that app could access or might access in the future. With the benefit of hindsight, we wish we had notified people whose information may have been impacted. Facebook has since notified all people potentially impacted with a detailed notice at the top of their News Feed.

221. How will we know on a quarterly basis if any corruption occurred?

Facebook's policies regarding third-party usage of its platform technologies have prohibited—and continue to prohibit—third-party app developers from selling or licensing user data obtained from Facebook and from sharing any user data obtained from Facebook with any ad network, data broker or other advertising or monetization-related service.

We use a variety of tools to enforce Facebook policies against violating parties, including developers. We review tens of thousands of apps per year and regularly disapprove noncompliant apps as part of our proactive review process. We also use tools like cease and desist letters, account suspensions, letter agreements, and civil litigation. For example, since 2006, Facebook

has sent over 1,150 cease-and-desist letters to over 1,600 targets. In 2017, we took action against about 370,000 apps, ranging from imposing certain restrictions to removal of the app from the platform. Moreover, we have required parties who have procured our data without authorization to delete that data. We have invested significant resources in these efforts.

Recently, we announced a number of additional steps we're taking to address concerns raised by Kogan's app.

- **Review our platform.** We will investigate all apps that had access to large amounts of data before the platform changes we announced in 2014, and we will audit any app where we identify suspicious activity. If we identify misuses of data, we'll take immediate action, including banning the app from our platform and pursuing legal action if appropriate.

- **Tell people about data misuse.** We will tell people about apps that have misused their data. This includes building a way for people to know if their data might have been accessed via the app. Moving forward, if we remove an app, we will tell people.

- **Turn off access for unused apps.** If someone has not used an app within the last three months, we will turn off the app's access to their data.

- **Restrict Facebook Login data.** We are changing Login, so that the only data that an app can request without app review will include name, profile photo, and email address. Requesting any other data will require approval from Facebook. We will also no longer allow apps to ask for access to information like religious or political views, relationship status and details, custom friends lists, education and work history, fitness activity, book reading and music listening activity, news reading, video watch activity, and games activity. We will encourage people to manage the apps they use. We already show people what apps their accounts are connected to and allow them to control what data they've permitted those apps to use. But we're making it easier for people to see what apps they use and the information they have shared with those apps.

- **Reward people who find vulnerabilities.** We launched the Data Abuse Bounty program so that people can report to us any misuses of data by app developers.

- **Update our policies.** We have updated our terms and Data Policy to explain how we use data and how data is shared with app developers.

222. When did you learn that FB could be manipulated for 'psy-ops' purposes, and what did you then do?

Facebook's policies regarding third-party usage of its platform technologies have prohibited—and continue to prohibit—third-party app developers from selling or licensing user data accessed from Facebook and from sharing any user data accessed from Facebook with any ad network, data broker or other advertising or monetization-related service. We take action on potential violations of our Platform Policies based on proactive review, external reports, and

other signals. Kogan was not permitted to sell or transfer data to third-parties for the purposes he did. In doing so, Kogan and his company violated Facebook's Platform Policies.

On December 11, 2015, *The Guardian* published an article reporting that Kogan and his company, GSR, may have passed information the app had obtained from Facebook users to SCL Elections Ltd. (SCL)/Cambridge Analytica. Facebook immediately banned Kogan's app from our platform and investigated what happened and what further action Facebook should take to enforce our Platform Policies. Facebook considered the matter closed after obtaining written certifications and confirmations from Kogan, GSR, Cambridge Analytica, and SCL declaring that all such data they had obtained was accounted for and destroyed. We did not have any reason to affirmatively question the veracity of any of these certifications until March 2018, when we learned from media reporting that questions had been raised concerning the accuracy of the certifications. Facebook immediately banned Cambridge Analytica and SCL from purchasing advertisements on our services as well as removed the personal accounts of some of their officers. Moreover, while Facebook's policies in place at the time allowed us to audit apps to ensure that they were safe and did not violate its terms, we had already terminated Kogan's app's access to Facebook. Accordingly, there were no ongoing concerns about the level of data that app could access or might access in the future. With the benefit of hindsight, we wish we had notified people whose information may have been impacted. Facebook has since notified all people potentially impacted with a detailed notice at the top of their News Feed.

223. Please ask why FB's Consent Decree didn't deter the Cambridge breach, ??U!

Facebook's policies regarding third-party usage of its platform technologies have prohibited—and continue to prohibit—third-party app developers from selling or licensing user data accessed from Facebook and from sharing any user data accessed from Facebook with any ad network, data broker or other advertising or monetization-related service. We take action on potential violations of our Platform Policies based on proactive review, external reports, and other signals. Kogan was not permitted to sell or transfer data to third-parties for the purposes he did. In doing so, Kogan and his company violated Facebook's Platform Policies.

On December 11, 2015, *The Guardian* published an article reporting that Kogan and his company, GSR, may have passed information the app had obtained from Facebook users to SCL Elections Ltd. (SCL)/Cambridge Analytica. Facebook immediately banned Kogan's app from our platform and investigated what happened and what further action Facebook should take to enforce our Platform Policies. Facebook considered the matter closed after obtaining written certifications and confirmations from Kogan, GSR, Cambridge Analytica, and SCL declaring that all such data they had obtained was accounted for and destroyed. We did not have any reason to affirmatively question the veracity of any of these certifications until March 2018, when we learned from media reporting that questions had been raised concerning the accuracy of the certifications. Facebook immediately banned Cambridge Analytica and SCL from purchasing advertisements on our services as well as removed the personal accounts of some of their officers. Moreover, while Facebook's policies in place at the time allowed us to audit apps to ensure that they were safe and did not violate its terms, we had already terminated Kogan's app's access to Facebook. Accordingly, there were no ongoing concerns about the level of data that app could access or might access in the future. With the benefit of hindsight, we wish we had

notified people whose information may have been impacted. Facebook has since notified all people potentially impacted with a detailed notice at the top of their News Feed.

224. Why did it take so long to notify users?

Facebook's policies regarding third-party usage of its platform technologies have prohibited—and continue to prohibit—third-party app developers from selling or licensing user data accessed from Facebook and from sharing any user data accessed from Facebook with any ad network, data broker or other advertising or monetization-related service. We take action on potential violations of our Platform Policies based on proactive review, external reports, and other signals. Kogan was not permitted to sell or transfer data to third-parties for the purposes he did. In doing so, Kogan and his company violated Facebook's Platform Policies.

On December 11, 2015, *The Guardian* published an article reporting that Kogan and his company, GSR, may have passed information the app had obtained from Facebook users to SCL Elections Ltd. (SCL)/Cambridge Analytica. Facebook immediately banned Kogan's app from our platform and investigated what happened and what further action Facebook should take to enforce our Platform Policies. Facebook considered the matter closed after obtaining written certifications and confirmations from Kogan, GSR, Cambridge Analytica, and SCL declaring that all such data they had obtained was accounted for and destroyed. We did not have any reason to affirmatively question the veracity of any of these certifications until March 2018, when we learned from media reporting that questions had been raised concerning the accuracy of the certifications. Facebook immediately banned Cambridge Analytica and SCL from purchasing advertisements on our services as well as removed the personal accounts of some of their officers. Moreover, while Facebook's policies in place at the time allowed us to audit apps to ensure that they were safe and did not violate its terms, we had already terminated Kogan's app's access to Facebook. Accordingly, there were no ongoing concerns about the level of data that app could access or might access in the future. With the benefit of hindsight, we wish we had notified people whose information may have been impacted. Facebook has since notified all people potentially impacted with a detailed notice at the top of their News Feed.

225. Describe their vetting system that allowed the researcher to gain access to so much of Facebook.

Facebook's policies regarding third-party usage of its platform technologies have prohibited—and continue to prohibit—third-party app developers from selling or licensing user data accessed from Facebook and from sharing any user data accessed from Facebook with any ad network, data broker or other advertising or monetization-related service. We take action on potential violations of our Platform Policies based on proactive review, external reports, and other signals. Kogan was not permitted to sell or transfer data to third-parties for the purposes he did. In doing so, Kogan and his company violated Facebook's Platform Policies.

On December 11, 2015, *The Guardian* published an article reporting that Kogan and his company, GSR, may have passed information the app had obtained from Facebook users to SCL Elections Ltd. (SCL)/Cambridge Analytica. Facebook immediately banned Kogan's app from our platform and investigated what happened and what further action Facebook should take to enforce our Platform Policies. Facebook considered the matter closed after obtaining written

certifications and confirmations from Kogan, GSR, Cambridge Analytica, and SCL declaring that all such data they had obtained was accounted for and destroyed. We did not have any reason to affirmatively question the veracity of any of these certifications until March 2018, when we learned from media reporting that questions had been raised concerning the accuracy of the certifications. Facebook immediately banned Cambridge Analytica and SCL from purchasing advertisements on our services as well as removed the personal accounts of some of their officers. Moreover, while Facebook's policies in place at the time allowed us to audit apps to ensure that they were safe and did not violate its terms, we had already terminated Kogan's app's access to Facebook. Accordingly, there were no ongoing concerns about the level of data that app could access or might access in the future. With the benefit of hindsight, we wish we had notified people whose information may have been impacted. Facebook has since notified all people potentially impacted with a detailed notice at the top of their News Feed.

226. When you learned that Cambridge Analytica's research project was actually for targeted psychographic political campaign work, did you contact the CEO immediately?

Facebook's policies regarding third-party usage of its platform technologies have prohibited—and continue to prohibit—third-party app developers from selling or licensing user data accessed from Facebook and from sharing any user data accessed from Facebook with any ad network, data broker or other advertising or monetization-related service. We take action on potential violations of our Platform Policies based on proactive review, external reports, and other signals. Kogan was not permitted to sell or transfer data to third-parties for the purposes he did. In doing so, Kogan and his company violated Facebook's Platform Policies.

On December 11, 2015, *The Guardian* published an article reporting that Kogan and his company, GSR, may have passed information the app had obtained from Facebook users to SCL Elections Ltd. (SCL)/Cambridge Analytica. Facebook immediately banned Kogan's app from our platform and investigated what happened and what further action Facebook should take to enforce our Platform Policies. Facebook considered the matter closed after obtaining written certifications and confirmations from Kogan, GSR, Cambridge Analytica, and SCL declaring that all such data they had obtained was accounted for and destroyed. We did not have any reason to affirmatively question the veracity of any of these certifications until March 2018, when we learned from media reporting that questions had been raised concerning the accuracy of the certifications. Facebook immediately banned Cambridge Analytica and SCL from purchasing advertisements on our services as well as removed the personal accounts of some of their officers. Moreover, while Facebook's policies in place at the time allowed us to audit apps to ensure that they were safe and did not violate its terms, we had already terminated Kogan's app's access to Facebook. Accordingly, there were no ongoing concerns about the level of data that app could access or might access in the future. With the benefit of hindsight, we wish we had notified people whose information may have been impacted. Facebook has since notified all people potentially impacted with a detailed notice at the top of their News Feed.

227. Did Cambridge Analytical breach the terms of their agreement with Facebook and if so what action is being taken.

Facebook's policies regarding third-party usage of its platform technologies have prohibited—and continue to prohibit—third-party app developers from selling or licensing user data accessed from Facebook and from sharing any user data accessed from Facebook with any ad network, data broker or other advertising or monetization-related service. We take action on potential violations of our Platform Policies based on proactive review, external reports, and other signals. Kogan was not permitted to sell or transfer data to third-parties for the purposes he did. In doing so, Kogan and his company violated Facebook's Platform Policies.

On December 11, 2015, *The Guardian* published an article reporting that Kogan and his company, GSR, may have passed information the app had obtained from Facebook users to SCL Elections Ltd. (SCL)/Cambridge Analytica. Facebook immediately banned Kogan's app from our platform and investigated what happened and what further action Facebook should take to enforce our Platform Policies. Facebook considered the matter closed after obtaining written certifications and confirmations from Kogan, GSR, Cambridge Analytica, and SCL declaring that all such data they had obtained was accounted for and destroyed. We did not have any reason to affirmatively question the veracity of any of these certifications until March 2018, when we learned from media reporting that questions had been raised concerning the accuracy of the certifications. Facebook immediately banned Cambridge Analytica and SCL from purchasing advertisements on our services as well as removed the personal accounts of some of their officers. Moreover, while Facebook's policies in place at the time allowed us to audit apps to ensure that they were safe and did not violate its terms, we had already terminated Kogan's app's access to Facebook. Accordingly, there were no ongoing concerns about the level of data that app could access or might access in the future. With the benefit of hindsight, we wish we had notified people whose information may have been impacted. Facebook has since notified all people potentially impacted with a detailed notice at the top of their News Feed.

228. What did you know? And when did you know?

Facebook's policies regarding third-party usage of its platform technologies have prohibited—and continue to prohibit—third-party app developers from selling or licensing user data accessed from Facebook and from sharing any user data accessed from Facebook with any ad network, data broker or other advertising or monetization-related service. We take action on potential violations of our Platform Policies based on proactive review, external reports, and other signals. Kogan was not permitted to sell or transfer data to third-parties for the purposes he did. In doing so, Kogan and his company violated Facebook's Platform Policies.

On December 11, 2015, *The Guardian* published an article reporting that Kogan and his company, GSR, may have passed information the app had obtained from Facebook users to SCL Elections Ltd. (SCL)/Cambridge Analytica. Facebook immediately banned Kogan's app from our platform and investigated what happened and what further action Facebook should take to enforce our Platform Policies. Facebook considered the matter closed after obtaining written certifications and confirmations from Kogan, GSR, Cambridge Analytica, and SCL declaring that all such data they had obtained was accounted for and destroyed. We did not have any reason to affirmatively question the veracity of any of these certifications until March 2018, when we learned from media reporting that questions had been raised concerning the accuracy of the certifications. Facebook immediately banned Cambridge Analytica and SCL from purchasing advertisements on our services as well as removed the personal accounts of some of their

officers. Moreover, while Facebook's policies in place at the time allowed us to audit apps to ensure that they were safe and did not violate its terms, we had already terminated Kogan's app's access to Facebook. Accordingly, there were no ongoing concerns about the level of data that app could access or might access in the future. With the benefit of hindsight, we wish we had notified people whose information may have been impacted. Facebook has since notified all people potentially impacted with a detailed notice at the top of their News Feed.

229. Why did you allow them to get/buy these files?

Facebook's policies regarding third-party usage of its platform technologies have prohibited—and continue to prohibit—third-party app developers from selling or licensing user data accessed from Facebook and from sharing any user data accessed from Facebook with any ad network, data broker or other advertising or monetization-related service. We take action on potential violations of our Platform Policies based on proactive review, external reports, and other signals. Kogan was not permitted to sell or transfer data to third-parties for the purposes he did. In doing so, Kogan and his company violated Facebook's Platform Policies.

On December 11, 2015, *The Guardian* published an article reporting that Kogan and his company, GSR, may have passed information the app had obtained from Facebook users to SCL Elections Ltd. (SCL)/Cambridge Analytica. Facebook immediately banned Kogan's app from our platform and investigated what happened and what further action Facebook should take to enforce our Platform Policies. Facebook considered the matter closed after obtaining written certifications and confirmations from Kogan, GSR, Cambridge Analytica, and SCL declaring that all such data they had obtained was accounted for and destroyed. We did not have any reason to affirmatively question the veracity of any of these certifications until March 2018, when we learned from media reporting that questions had been raised concerning the accuracy of the certifications. Facebook immediately banned Cambridge Analytica and SCL from purchasing advertisements on our services as well as removed the personal accounts of some of their officers. Moreover, while Facebook's policies in place at the time allowed us to audit apps to ensure that they were safe and did not violate its terms, we had already terminated Kogan's app's access to Facebook. Accordingly, there were no ongoing concerns about the level of data that app could access or might access in the future. With the benefit of hindsight, we wish we had notified people whose information may have been impacted. Facebook has since notified all people potentially impacted with a detailed notice at the top of their News Feed.

230. Were Facebook people working with Cambridge Analytica and the Trump Campaign to set up targeted messaging?

a. What is their accountability? They need to change their business model of making money off of the user's data.

b. What are the safeguards they are instituting? -we need oversight to ensure this does not happen again.

Facebook's policies regarding third-party usage of its platform technologies have prohibited—and continue to prohibit—third-party app developers from selling or licensing user data accessed from Facebook and from sharing any user data accessed from Facebook with any

ad network, data broker or other advertising or monetization-related service. We take action on potential violations of our Platform Policies based on proactive review, external reports, and other signals. Kogan was not permitted to sell or transfer data to third-parties for the purposes he did. In doing so, Kogan and his company violated Facebook's Platform Policies.

On December 11, 2015, *The Guardian* published an article reporting that Kogan and his company, GSR, may have passed information the app had obtained from Facebook users to SCL Elections Ltd. (SCL)/Cambridge Analytica. Facebook immediately banned Kogan's app from our platform and investigated what happened and what further action Facebook should take to enforce our Platform Policies. Facebook considered the matter closed after obtaining written certifications and confirmations from Kogan, GSR, Cambridge Analytica, and SCL declaring that all such data they had obtained was accounted for and destroyed. We did not have any reason to affirmatively question the veracity of any of these certifications until March 2018, when we learned from media reporting that questions had been raised concerning the accuracy of the certifications. Facebook immediately banned Cambridge Analytica and SCL from purchasing advertisements on our services as well as removed the personal accounts of some of their officers. Moreover, while Facebook's policies in place at the time allowed us to audit apps to ensure that they were safe and did not violate its terms, we had already terminated Kogan's app's access to Facebook. Accordingly, there were no ongoing concerns about the level of data that app could access or might access in the future. With the benefit of hindsight, we wish we had notified people whose information may have been impacted. Facebook has since notified all people potentially impacted with a detailed notice at the top of their News Feed.

231. Facebook was aware of the issue for two years. It was brought to light by someone other than Facebook. Why didn't Facebook let their users know of the breech?

Facebook's policies regarding third-party usage of its platform technologies have prohibited—and continue to prohibit—third-party app developers from selling or licensing user data accessed from Facebook and from sharing any user data accessed from Facebook with any ad network, data broker or other advertising or monetization-related service. We take action on potential violations of our Platform Policies based on proactive review, external reports, and other signals. Kogan was not permitted to sell or transfer data to third-parties for the purposes he did. In doing so, Kogan and his company violated Facebook's Platform Policies.

On December 11, 2015, *The Guardian* published an article reporting that Kogan and his company, GSR, may have passed information the app had obtained from Facebook users to SCL Elections Ltd. (SCL)/Cambridge Analytica. Facebook immediately banned Kogan's app from our platform and investigated what happened and what further action Facebook should take to enforce our Platform Policies. Facebook considered the matter closed after obtaining written certifications and confirmations from Kogan, GSR, Cambridge Analytica, and SCL declaring that all such data they had obtained was accounted for and destroyed. We did not have any reason to affirmatively question the veracity of any of these certifications until March 2018, when we learned from media reporting that questions had been raised concerning the accuracy of the certifications. Facebook immediately banned Cambridge Analytica and SCL from purchasing advertisements on our services as well as removed the personal accounts of some of their officers. Moreover, while Facebook's policies in place at the time allowed us to audit apps to ensure that they were safe and did not violate its terms, we had already terminated Kogan's app's

access to Facebook. Accordingly, there were no ongoing concerns about the level of data that app could access or might access in the future. With the benefit of hindsight, we wish we had notified people whose information may have been impacted. Facebook has since notified all people potentially impacted with a detailed notice at the top of their News Feed.

232. How did this security breach happen, was it just to get dollars?

Facebook's policies regarding third-party usage of its platform technologies have prohibited—and continue to prohibit—third-party app developers from selling or licensing user data accessed from Facebook and from sharing any user data accessed from Facebook with any ad network, data broker or other advertising or monetization-related service. We take action on potential violations of our Platform Policies based on proactive review, external reports, and other signals. Kogan was not permitted to sell or transfer data to third-parties for the purposes he did. In doing so, Kogan and his company violated Facebook's Platform Policies.

On December 11, 2015, *The Guardian* published an article reporting that Kogan and his company, GSR, may have passed information the app had obtained from Facebook users to SCL Elections Ltd. (SCL)/Cambridge Analytica. Facebook immediately banned Kogan's app from our platform and investigated what happened and what further action Facebook should take to enforce our Platform Policies. Facebook considered the matter closed after obtaining written certifications and confirmations from Kogan, GSR, Cambridge Analytica, and SCL declaring that all such data they had obtained was accounted for and destroyed. We did not have any reason to affirmatively question the veracity of any of these certifications until March 2018, when we learned from media reporting that questions had been raised concerning the accuracy of the certifications. Facebook immediately banned Cambridge Analytica and SCL from purchasing advertisements on our services as well as removed the personal accounts of some of their officers. Moreover, while Facebook's policies in place at the time allowed us to audit apps to ensure that they were safe and did not violate its terms, we had already terminated Kogan's app's access to Facebook. Accordingly, there were no ongoing concerns about the level of data that app could access or might access in the future. With the benefit of hindsight, we wish we had notified people whose information may have been impacted. Facebook has since notified all people potentially impacted with a detailed notice at the top of their News Feed.

233. Why did Facebook decide not to let its users know while knowing it in 2016 or maybe even earlier?

Facebook's policies regarding third-party usage of its platform technologies have prohibited—and continue to prohibit—third-party app developers from selling or licensing user data accessed from Facebook and from sharing any user data accessed from Facebook with any ad network, data broker or other advertising or monetization-related service. We take action on potential violations of our Platform Policies based on proactive review, external reports, and other signals. Kogan was not permitted to sell or transfer data to third-parties for the purposes he did. In doing so, Kogan and his company violated Facebook's Platform Policies.

On December 11, 2015, *The Guardian* published an article reporting that Kogan and his company, GSR, may have passed information the app had obtained from Facebook users to SCL Elections Ltd. (SCL)/Cambridge Analytica. Facebook immediately banned Kogan's app from

our platform and investigated what happened and what further action Facebook should take to enforce our Platform Policies. Facebook considered the matter closed after obtaining written certifications and confirmations from Kogan, GSR, Cambridge Analytica, and SCL declaring that all such data they had obtained was accounted for and destroyed. We did not have any reason to affirmatively question the veracity of any of these certifications until March 2018, when we learned from media reporting that questions had been raised concerning the accuracy of the certifications. Facebook immediately banned Cambridge Analytica and SCL from purchasing advertisements on our services as well as removed the personal accounts of some of their officers. Moreover, while Facebook's policies in place at the time allowed us to audit apps to ensure that they were safe and did not violate its terms, we had already terminated Kogan's app's access to Facebook. Accordingly, there were no ongoing concerns about the level of data that app could access or might access in the future. With the benefit of hindsight, we wish we had notified people whose information may have been impacted. Facebook has since notified all people potentially impacted with a detailed notice at the top of their News Feed.

234. Did you release the original data to the researcher with personal names and if so why?

Facebook's policies regarding third-party usage of its platform technologies have prohibited—and continue to prohibit—third-party app developers from selling or licensing user data accessed from Facebook and from sharing any user data accessed from Facebook with any ad network, data broker or other advertising or monetization-related service. We take action on potential violations of our Platform Policies based on proactive review, external reports, and other signals. Kogan was not permitted to sell or transfer data to third-parties for the purposes he did. In doing so, Kogan and his company violated Facebook's Platform Policies.

On December 11, 2015, *The Guardian* published an article reporting that Kogan and his company, GSR, may have passed information the app had obtained from Facebook users to SCL Elections Ltd. (SCL)/Cambridge Analytica. Facebook immediately banned Kogan's app from our platform and investigated what happened and what further action Facebook should take to enforce our Platform Policies. Facebook considered the matter closed after obtaining written certifications and confirmations from Kogan, GSR, Cambridge Analytica, and SCL declaring that all such data they had obtained was accounted for and destroyed. We did not have any reason to affirmatively question the veracity of any of these certifications until March 2018, when we learned from media reporting that questions had been raised concerning the accuracy of the certifications. Facebook immediately banned Cambridge Analytica and SCL from purchasing advertisements on our services as well as removed the personal accounts of some of their officers. Moreover, while Facebook's policies in place at the time allowed us to audit apps to ensure that they were safe and did not violate its terms, we had already terminated Kogan's app's access to Facebook. Accordingly, there were no ongoing concerns about the level of data that app could access or might access in the future. With the benefit of hindsight, we wish we had notified people whose information may have been impacted. Facebook has since notified all people potentially impacted with a detailed notice at the top of their News Feed.

235. Why was a written "We deleted the data" enough from those who took it illegally?

Facebook's policies regarding third-party usage of its platform technologies have prohibited—and continue to prohibit—third-party app developers from selling or licensing user data accessed from Facebook and from sharing any user data accessed from Facebook with any ad network, data broker or other advertising or monetization-related service. We take action on potential violations of our Platform Policies based on proactive review, external reports, and other signals. Kogan was not permitted to sell or transfer data to third-parties for the purposes he did. In doing so, Kogan and his company violated Facebook's Platform Policies.

On December 11, 2015, *The Guardian* published an article reporting that Kogan and his company, GSR, may have passed information the app had obtained from Facebook users to SCL Elections Ltd. (SCL)/Cambridge Analytica. Facebook immediately banned Kogan's app from our platform and investigated what happened and what further action Facebook should take to enforce our Platform Policies. Facebook considered the matter closed after obtaining written certifications and confirmations from Kogan, GSR, Cambridge Analytica, and SCL declaring that all such data they had obtained was accounted for and destroyed. We did not have any reason to affirmatively question the veracity of any of these certifications until March 2018, when we learned from media reporting that questions had been raised concerning the accuracy of the certifications. Facebook immediately banned Cambridge Analytica and SCL from purchasing advertisements on our services as well as removed the personal accounts of some of their officers. Moreover, while Facebook's policies in place at the time allowed us to audit apps to ensure that they were safe and did not violate its terms, we had already terminated Kogan's app's access to Facebook. Accordingly, there were no ongoing concerns about the level of data that app could access or might access in the future. With the benefit of hindsight, we wish we had notified people whose information may have been impacted. Facebook has since notified all people potentially impacted with a detailed notice at the top of their News Feed.

236. What other organizations have accessed Facebook users' account information?

We believe everyone deserves good privacy controls. A user owns the information they share on Facebook. This means they decide what they share and who they share it with on Facebook, and they can change their mind. We require websites and apps who use our tools to tell users they're collecting and sharing their information with us, and to get users' permission to do so.

Everyone has the right to expect strong protections for their information. We also need to do our part to help keep our community safe, in a way that's consistent with people's privacy expectations. We've recently announced several steps to give people more control over their privacy, including a new Privacy Shortcuts tool that we're rolling out now to give people information about how to control their information, including choosing who can see what they post and adding protections like two-factor authentication to their account. People can learn more about how to protect their privacy in our updated Data Policy and in our Privacy Basics feature (https://www.facebook.com/about/basics).

We are in the process of investigating every app that had access to a large amount of information before we changed our Platform in 2014. The investigation process is in full swing. We have large teams of internal and external experts working hard to investigate these apps as quickly as possible. As of early June 2018, thousands of apps have been investigated and around

200 apps have been suspended—pending a thorough investigation into whether they did in fact misuse any data. Where we find evidence that these or other apps did misuse data, we will ban them and let people know.

Facebook is generally not opposed to regulation but wants to ensure it is the right regulation. The issues facing the industry are complex, multi-faceted, and affect an important part of peoples' lives. As such, Facebook is absolutely committed to working with regulators, like Congress, to craft the right regulations. Facebook would be happy to review any proposed legislation and provide comments.

237. Why did it take so long for you to acknowledge the problem and now what are you going to do to fix??

Facebook's policies regarding third-party usage of its platform technologies have prohibited—and continue to prohibit—third-party app developers from selling or licensing user data accessed from Facebook and from sharing any user data accessed from Facebook with any ad network, data broker or other advertising or monetization-related service. We take action on potential violations of our Platform Policies based on proactive review, external reports, and other signals. Kogan was not permitted to sell or transfer data to third-parties for the purposes he did. In doing so, Kogan and his company violated Facebook's Platform Policies.

On December 11, 2015, *The Guardian* published an article reporting that Kogan and his company, GSR, may have passed information the app had obtained from Facebook users to SCL Elections Ltd. (SCL)/Cambridge Analytica. Facebook immediately banned Kogan's app from our platform and investigated what happened and what further action Facebook should take to enforce our Platform Policies. Facebook considered the matter closed after obtaining written certifications and confirmations from Kogan, GSR, Cambridge Analytica, and SCL declaring that all such data they had obtained was accounted for and destroyed. We did not have any reason to affirmatively question the veracity of any of these certifications until March 2018, when we learned from media reporting that questions had been raised concerning the accuracy of the certifications. Facebook immediately banned Cambridge Analytica and SCL from purchasing advertisements on our services as well as removed the personal accounts of some of their officers. Moreover, while Facebook's policies in place at the time allowed us to audit apps to ensure that they were safe and did not violate its terms, we had already terminated Kogan's app's access to Facebook. Accordingly, there were no ongoing concerns about the level of data that app could access or might access in the future. With the benefit of hindsight, we wish we had notified people whose information may have been impacted. Facebook has since notified all people potentially impacted with a detailed notice at the top of their News Feed.

238. When did you know and exactly what did you do?

Facebook's policies regarding third-party usage of its platform technologies have prohibited—and continue to prohibit—third-party app developers from selling or licensing user data accessed from Facebook and from sharing any user data accessed from Facebook with any ad network, data broker or other advertising or monetization-related service. We take action on potential violations of our Platform Policies based on proactive review, external reports, and

other signals. Kogan was not permitted to sell or transfer data to third-parties for the purposes he did. In doing so, Kogan and his company violated Facebook's Platform Policies.

On December 11, 2015, *The Guardian* published an article reporting that Kogan and his company, GSR, may have passed information the app had obtained from Facebook users to SCL Elections Ltd. (SCL)/Cambridge Analytica. Facebook immediately banned Kogan's app from our platform and investigated what happened and what further action Facebook should take to enforce our Platform Policies. Facebook considered the matter closed after obtaining written certifications and confirmations from Kogan, GSR, Cambridge Analytica, and SCL declaring that all such data they had obtained was accounted for and destroyed. We did not have any reason to affirmatively question the veracity of any of these certifications until March 2018, when we learned from media reporting that questions had been raised concerning the accuracy of the certifications. Facebook immediately banned Cambridge Analytica and SCL from purchasing advertisements on our services as well as removed the personal accounts of some of their officers. Moreover, while Facebook's policies in place at the time allowed us to audit apps to ensure that they were safe and did not violate its terms, we had already terminated Kogan's app's access to Facebook. Accordingly, there were no ongoing concerns about the level of data that app could access or might access in the future. With the benefit of hindsight, we wish we had notified people whose information may have been impacted. Facebook has since notified all people potentially impacted with a detailed notice at the top of their News Feed.

239. Who has been damaged because of your company's practices?

Facebook's policies regarding third-party usage of its platform technologies have prohibited—and continue to prohibit—third-party app developers from selling or licensing user data accessed from Facebook and from sharing any user data accessed from Facebook with any ad network, data broker or other advertising or monetization-related service. We take action on potential violations of our Platform Policies based on proactive review, external reports, and other signals. Kogan was not permitted to sell or transfer data to third-parties for the purposes he did. In doing so, Kogan and his company violated Facebook's Platform Policies.

On December 11, 2015, *The Guardian* published an article reporting that Kogan and his company, GSR, may have passed information the app had obtained from Facebook users to SCL Elections Ltd. (SCL)/Cambridge Analytica. Facebook immediately banned Kogan's app from our platform and investigated what happened and what further action Facebook should take to enforce our Platform Policies. Facebook considered the matter closed after obtaining written certifications and confirmations from Kogan, GSR, Cambridge Analytica, and SCL declaring that all such data they had obtained was accounted for and destroyed. We did not have any reason to affirmatively question the veracity of any of these certifications until March 2018, when we learned from media reporting that questions had been raised concerning the accuracy of the certifications. Facebook immediately banned Cambridge Analytica and SCL from purchasing advertisements on our services as well as removed the personal accounts of some of their officers. Moreover, while Facebook's policies in place at the time allowed us to audit apps to ensure that they were safe and did not violate its terms, we had already terminated Kogan's app's access to Facebook. Accordingly, there were no ongoing concerns about the level of data that app could access or might access in the future. With the benefit of hindsight, we wish we had

notified people whose information may have been impacted. Facebook has since notified all people potentially impacted with a detailed notice at the top of their News Feed.

240. Why does Facebook take so long (years) to notify folks that their data has been stolen and misused?

Facebook's policies regarding third-party usage of its platform technologies have prohibited—and continue to prohibit—third-party app developers from selling or licensing user data accessed from Facebook and from sharing any user data accessed from Facebook with any ad network, data broker or other advertising or monetization-related service. We take action on potential violations of our Platform Policies based on proactive review, external reports, and other signals. Kogan was not permitted to sell or transfer data to third-parties for the purposes he did. In doing so, Kogan and his company violated Facebook's Platform Policies.

On December 11, 2015, *The Guardian* published an article reporting that Kogan and his company, GSR, may have passed information the app had obtained from Facebook users to SCL Elections Ltd. (SCL)/Cambridge Analytica. Facebook immediately banned Kogan's app from our platform and investigated what happened and what further action Facebook should take to enforce our Platform Policies. Facebook considered the matter closed after obtaining written certifications and confirmations from Kogan, GSR, Cambridge Analytica, and SCL declaring that all such data they had obtained was accounted for and destroyed. We did not have any reason to affirmatively question the veracity of any of these certifications until March 2018, when we learned from media reporting that questions had been raised concerning the accuracy of the certifications. Facebook immediately banned Cambridge Analytica and SCL from purchasing advertisements on our services as well as removed the personal accounts of some of their officers. Moreover, while Facebook's policies in place at the time allowed us to audit apps to ensure that they were safe and did not violate its terms, we had already terminated Kogan's app's access to Facebook. Accordingly, there were no ongoing concerns about the level of data that app could access or might access in the future. With the benefit of hindsight, we wish we had notified people whose information may have been impacted. Facebook has since notified all people potentially impacted with a detailed notice at the top of their News Feed.

241. Was Mr. Zuckerberg's data included in the data sold to the malicious third parties?

Facebook's policies regarding third-party usage of its platform technologies have prohibited—and continue to prohibit—third-party app developers from selling or licensing user data accessed from Facebook and from sharing any user data accessed from Facebook with any ad network, data broker or other advertising or monetization-related service. We take action on potential violations of our Platform Policies based on proactive review, external reports, and other signals. Kogan was not permitted to sell or transfer data to third-parties for the purposes he did. In doing so, Kogan and his company violated Facebook's Platform Policies.

On December 11, 2015, *The Guardian* published an article reporting that Kogan and his company, GSR, may have passed information the app had obtained from Facebook users to SCL Elections Ltd. (SCL)/Cambridge Analytica. Facebook immediately banned Kogan's app from our platform and investigated what happened and what further action Facebook should take to enforce our Platform Policies. Facebook considered the matter closed after obtaining written

certifications and confirmations from Kogan, GSR, Cambridge Analytica, and SCL declaring that all such data they had obtained was accounted for and destroyed. We did not have any reason to affirmatively question the veracity of any of these certifications until March 2018, when we learned from media reporting that questions had been raised concerning the accuracy of the certifications. Facebook immediately banned Cambridge Analytica and SCL from purchasing advertisements on our services as well as removed the personal accounts of some of their officers. Moreover, while Facebook's policies in place at the time allowed us to audit apps to ensure that they were safe and did not violate its terms, we had already terminated Kogan's app's access to Facebook. Accordingly, there were no ongoing concerns about the level of data that app could access or might access in the future. With the benefit of hindsight, we wish we had notified people whose information may have been impacted. Facebook has since notified all people potentially impacted with a detailed notice at the top of their News Feed.

242. What went wrong and what can Facebook do to assure its customers have privacy?

We believe everyone deserves good privacy controls. A user owns the information they share on Facebook. This means they decide what they share and who they share it with on Facebook, and they can change their mind. We require websites and apps who use our tools to tell users they're collecting and sharing their information with us, and to get users' permission to do so.

Everyone has the right to expect strong protections for their information. We also need to do our part to help keep our community safe, in a way that's consistent with people's privacy expectations. We've recently announced several steps to give people more control over their privacy, including a new Privacy Shortcuts tool that we're rolling out now to give people information about how to control their information, including choosing who can see what they post and adding protections like two-factor authentication to their account. People can learn more about how to protect their privacy in our updated Data Policy and in our Privacy Basics feature (https://www.facebook.com/about/basics).

We are in the process of investigating every app that had access to a large amount of information before we changed our Platform in 2014. The investigation process is in full swing. We have large teams of internal and external experts working hard to investigate these apps as quickly as possible. As of early June 2018, thousands of apps have been investigated and around 200 apps have been suspended—pending a thorough investigation into whether they did in fact misuse any data. Where we find evidence that these or other apps did misuse data, we will ban them and let people know.

Facebook is generally not opposed to regulation but wants to ensure it is the right regulation. The issues facing the industry are complex, multi-faceted, and affect an important part of peoples' lives. As such, Facebook is absolutely committed to working with regulators, like Congress, to craft the right regulations. Facebook would be happy to review any proposed legislation and provide comments.

243. Did your relationship with your investor Yuri Milner influence your release of information to Cambridge Analytica and in selling hits to Russian hackers??? Rubles huh?

For years, we had been aware of other types of activity that appeared to come from Russian sources—largely traditional security threats such as attacking people's accounts or using social media platforms to spread stolen information. What we saw early in the 2016 campaign cycle followed this pattern. Our security team that focuses on threat intelligence—which investigates advanced security threats as part of our overall information security organization—was, from the outset, alert to the possibility of Russian activity. In several instances before November 8, 2016, this team detected and mitigated threats from actors with ties to Russia and reported them to US law enforcement officials. This included activity from a cluster of accounts we had assessed to belong to a group (APT28) that the US government has publicly linked to Russian military intelligence services. This activity, which was aimed at employees of major US political parties, fell into the normal categories of offensive cyber activities we monitor for. We warned the targets who were at highest risk, and were later in contact with law enforcement authorities about this activity.

Later in the summer we also started to see a new kind of behavior from APT28-related accounts—namely, the creation of fake personas that were then used to seed stolen information to journalists. These fake personas were organized under the banner of an organization that called itself DC Leaks. This activity violated our policies, and we removed the DC Leaks accounts.

Facebook learned from press accounts and statements by congressional leaders that Russian actors might have tried to interfere in the 2016 election by exploiting Facebook's ad tools. This is not something we had seen before, and so we started an investigation. We found that fake accounts associated with the IRA tried to influence the election.

This will never be a solved problem because we're up against determined, creative and well-funded adversaries. But we are making steady progress in preventing bad actors from using misinformation to undermine the democratic process, such as: increased ad transparency, advertiser verification and labeling, updating targeting criteria, better technological efforts to find and disable fake accounts, third-party fact checking to stop the spread of false news, doubling the number of people working on safety and security, greater industry collaboration, increased information sharing and reporting channels, proactive identification of election threats, and specific action against the Russia-based IRA.

We will continue to work with the government, and across the tech industry and civil society, to address this important national security matter so that we can do our part to prevent similar abuse from happening again.

244. **Will he guarantee that we will know as soon as he knows in the future?**

Facebook's policies regarding third-party usage of its platform technologies have prohibited—and continue to prohibit—third-party app developers from selling or licensing user data obtained from Facebook and from sharing any user data obtained from Facebook with any ad network, data broker or other advertising or monetization-related service.

We use a variety of tools to enforce Facebook policies against violating parties, including developers. We review tens of thousands of apps per year and regularly disapprove noncompliant

apps as part of our proactive review process. We also use tools like cease and desist letters, account suspensions, letter agreements, and civil litigation. For example, since 2006, Facebook has sent over 1,150 cease-and-desist letters to over 1,600 targets. In 2017, we took action against about 370,000 apps, ranging from imposing certain restrictions to removal of the app from the platform. Moreover, we have required parties who have procured our data without authorization to delete that data. We have invested significant resources in these efforts.

Recently, we announced a number of additional steps we're taking to address concerns raised by Kogan's app.

- **Review our platform.** We will investigate all apps that had access to large amounts of data before the platform changes we announced in 2014, and we will audit any app where we identify suspicious activity. If we identify misuses of data, we'll take immediate action, including banning the app from our platform and pursuing legal action if appropriate.

- **Tell people about data misuse.** We will tell people about apps that have misused their data. This includes building a way for people to know if their data might have been accessed via the app. Moving forward, if we remove an app, we will tell people.

- **Turn off access for unused apps.** If someone has not used an app within the last three months, we will turn off the app's access to their data.

- **Restrict Facebook Login data.** We are changing Login, so that the only data that an app can request without app review will include name, profile photo, and email address. Requesting any other data will require approval from Facebook. We will also no longer allow apps to ask for access to information like religious or political views, relationship status and details, custom friends lists, education and work history, fitness activity, book reading and music listening activity, news reading, video watch activity, and games activity. We will encourage people to manage the apps they use. We already show people what apps their accounts are connected to and allow them to control what data they've permitted those apps to use. But we're making it easier for people to see what apps they use and the information they have shared with those apps.

- **Reward people who find vulnerabilities.** We launched the Data Abuse Bounty program so that people can report to us any misuses of data by app developers.

- **Update our policies.** We have updated our terms and Data Policy to explain how we use data and how data is shared with app developers.

245. Why shouldn't government regulate your industry?

Protecting people's data is one of our most important responsibilities, and we are committed to continuing our work to improve how we protect people's information and to working with regulators to draft appropriate regulations. Our mission is to give people the power to build community and bring the world closer together. As the internet becomes more important

in people's lives, the real question is about the right set of regulations that should apply to all internet services, regardless of size. Across the board, we have a responsibility to not just build tools, but to make sure that they're used in ways that are positive for our users. Facebook is generally not opposed to regulation but wants to ensure it is the right regulation. The issues facing the industry are complex, multi-faceted, and affect an important part of peoples' lives. As such, Facebook is absolutely committed to working with regulators, like Congress, to craft the right regulations.

We are already regulated in many ways—for example, under the Federal Trade Commission Act—and we are subject to ongoing oversight by the FTC under the terms of a 2011 consent order. We furnished extensive information to the FTC regarding the ability for users to port their Facebook data (including friends data that had been shared with them) with apps on Facebook's platform, as part of the FTC's investigation culminating in the July 27, 2012 Consent Order. The Consent Order memorializes the agreement between Facebook and the FTC and did not require Facebook to turn off or change the ability for people to port friends data that had been shared with them on Facebook to apps they used. Facebook voluntarily changed this feature of Platform in 2014, however. Facebook has not violated the Federal Trade Commission Act. Facebook is not in a position to determine whether third-party app developers violated the Act and leaves that determination to the FTC, although we can confirm that misrepresenting the terms of an app to users is a violation of Facebook's developer policies.

Facebook has inherent incentives to protect its customers' privacy and address breaches and vulnerabilities. Indeed, the recent discovery of misconduct by an app developer on the Facebook platform clearly hurt Facebook and made it harder for us to achieve our social mission. As such, Facebook is committed to protecting our platform from bad actors, ensuring we are able to continue our mission of giving people a voice and bringing them closer together. It will take some time to work through all the changes we need to make across the company, but Facebook is committed to getting this right.

246. FACEBOOK SHOULD BE SUBJECT TO THE SAME REQUIREMENTS AS BROADCAST MEDIA IS WHEN ACCEPTING ADVERTISING

Protecting people's data is one of our most important responsibilities, and we are committed to continuing our work to improve how we protect people's information and to working with regulators to draft appropriate regulations. Our mission is to give people the power to build community and bring the world closer together. As the internet becomes more important in people's lives, the real question is about the right set of regulations that should apply to all internet services, regardless of size. Across the board, we have a responsibility to not just build tools, but to make sure that they're used in ways that are positive for our users. Facebook is generally not opposed to regulation but wants to ensure it is the right regulation. The issues facing the industry are complex, multi-faceted, and affect an important part of peoples' lives. As such, Facebook is absolutely committed to working with regulators, like Congress, to craft the right regulations.

We are already regulated in many ways—for example, under the Federal Trade Commission Act—and we are subject to ongoing oversight by the FTC under the terms of a 2011 consent order. We furnished extensive information to the FTC regarding the ability for users to

port their Facebook data (including friends data that had been shared with them) with apps on Facebook's platform, as part of the FTC's investigation culminating in the July 27, 2012 Consent Order. The Consent Order memorializes the agreement between Facebook and the FTC and did not require Facebook to turn off or change the ability for people to port friends data that had been shared with them on Facebook to apps they used. Facebook voluntarily changed this feature of Platform in 2014, however. Facebook has not violated the Federal Trade Commission Act. Facebook is not in a position to determine whether third-party app developers violated the Act and leaves that determination to the FTC, although we can confirm that misrepresenting the terms of an app to users is a violation of Facebook's developer policies.

Facebook has inherent incentives to protect its customers' privacy and address breaches and vulnerabilities. Indeed, the recent discovery of misconduct by an app developer on the Facebook platform clearly hurt Facebook and made it harder for us to achieve our social mission. As such, Facebook is committed to protecting our platform from bad actors, ensuring we are able to continue our mission of giving people a voice and bringing them closer together. It will take some time to work through all the changes we need to make across the company, but Facebook is committed to getting this right.

247. Sen Mark Warner is supporting his bi partisan bill, Honest Ads Bill and had approached Zuckerberg several times about bill. Until now, Zuckerberg would not sign on to bill. Is he really ready to do so now and what will he do to follow up? Thanks so much for "grilling" him! (Fran Codispoti)

To build a secure product with extensive infrastructure that connects people wherever they live or whatever their income level, we need to make sure everyone can afford it. Advertising lets us keep Facebook free, which ensures it remains affordable for everyone. We also believe the ads you see across the Facebook family of apps and services should be useful and relevant to you. Users can't opt out of seeing ads altogether because selling ads is what keeps Facebook free, but they do have different options to control how their data can and can't be used to show them ads. They're all found in ad preferences, which allows users to turn off the use of all data collected from partners off Facebook to target ads. Users can also decide which of their profile fields they want used for ad targeting in the Information section under "About you." Users can remove themselves from interests under "Your interests" and categories under "Your categories." And, we do not sell people's information to anyone, and we never will.

Facebook is committed to transparency for all ads, including ads with political content. Facebook believes that people should be able to easily understand why they are seeing ads, who paid for them, and what other ads those advertisers are running. As such, Facebook only allows authorized advertisers to run ads about elections or issues that are being debated across the country. In order to be authorized by Facebook, advertisers will need to confirm their identity and location. Furthermore, all political and issue ads will include a disclosure which reads: "Paid for by," and when users click on this disclosure they will be able to see details about the advertiser. Users will also be able to see an explanation of why they saw the particular ad. This is similar to the disclosure included on political TV advertisements. We just launched globally View Active Ads, a feature that will enable anyone to see all of the ads an advertiser is currently running by visiting the advertiser's Facebook Page.

248. Why should Congress allow you to remain the Chairman and CEO of Facebook after you knowingly allowed your users private information to be scraped by Bad Actors and then after seeing it put to evil use did nothing!

We recognize that we have made mistakes, and we are committed to learning from this experience to secure our platform further and make our community safer for everyone going forward. As our CEO Mark Zuckerberg has said, when you are building something unprecedented like Facebook, there are going to be mistakes. What people should hold us accountable for is learning from the mistakes and continually doing better—and, at the end of the day, making sure that we're building things that people like and that make their lives better.

Particularly in the past few months, we've realized that we need to take a broader view of our responsibility to our community. Part of that effort is continuing our ongoing efforts to identify ways that we can improve our privacy practices. We've heard loud and clear that privacy settings and other important tools are too hard to find and that we must do more to keep people informed. So, we're taking additional steps to put people more in control of their privacy. For instance, we redesigned our entire settings menu on mobile devices from top to bottom to make things easier to find. We also created a new Privacy Shortcuts in a menu where users can control their data in just a few taps, with clearer explanations of how our controls work. The experience is now clearer, more visual, and easy-to-find. Furthermore, we also updated our terms of service that include our commitments to everyone using Facebook. We explain the services we offer in language that's easier to read. We've also updated our Data Policy to better spell out what data we collect and how we use it in Facebook, Instagram, Messenger, and other products.

249. How can Congress work with Tech firms to ensure safeguards to media accuracy and citizens' privacy?

We believe everyone deserves good privacy controls. A user owns the information they share on Facebook. This means they decide what they share and who they share it with on Facebook, and they can change their mind. We require websites and apps who use our tools to tell users they're collecting and sharing their information with us, and to get users' permission to do so.

Everyone has the right to expect strong protections for their information. We also need to do our part to help keep our community safe, in a way that's consistent with people's privacy expectations. We've recently announced several steps to give people more control over their privacy, including a new Privacy Shortcuts tool that we're rolling out now to give people information about how to control their information, including choosing who can see what they post and adding protections like two-factor authentication to their account. People can learn more about how to protect their privacy in our updated Data Policy and in our Privacy Basics feature (https://www.facebook.com/about/basics).

We are in the process of investigating every app that had access to a large amount of information before we changed our Platform in 2014. The investigation process is in full swing. We have large teams of internal and external experts working hard to investigate these apps as quickly as possible. As of early June 2018, thousands of apps have been investigated and around 200 apps have been suspended—pending a thorough investigation into whether they did in fact

misuse any data. Where we find evidence that these or other apps did misuse data, we will ban them and let people know.

Facebook is generally not opposed to regulation but wants to ensure it is the right regulation. The issues facing the industry are complex, multi-faceted, and affect an important part of peoples' lives. As such, Facebook is absolutely committed to working with regulators, like Congress, to craft the right regulations. Facebook would be happy to review any proposed legislation and provide comments.

250. How do you think tech companies should be held accountable through policy and federal regulation?

Protecting people's data is one of our most important responsibilities, and we are committed to continuing our work to improve how we protect people's information and to working with regulators to draft appropriate regulations. Our mission is to give people the power to build community and bring the world closer together. As the internet becomes more important in people's lives, the real question is about the right set of regulations that should apply to all internet services, regardless of size. Across the board, we have a responsibility to not just build tools, but to make sure that they're used in ways that are positive for our users. Facebook is generally not opposed to regulation but wants to ensure it is the right regulation. The issues facing the industry are complex, multi-faceted, and affect an important part of peoples' lives. As such, Facebook is absolutely committed to working with regulators, like Congress, to craft the right regulations.

We are already regulated in many ways—for example, under the Federal Trade Commission Act—and we are subject to ongoing oversight by the FTC under the terms of a 2011 consent order. We furnished extensive information to the FTC regarding the ability for users to port their Facebook data (including friends data that had been shared with them) with apps on Facebook's platform, as part of the FTC's investigation culminating in the July 27, 2012 Consent Order. The Consent Order memorializes the agreement between Facebook and the FTC and did not require Facebook to turn off or change the ability for people to port friends data that had been shared with them on Facebook to apps they used. Facebook voluntarily changed this feature of Platform in 2014, however. Facebook has not violated the Federal Trade Commission Act. Facebook is not in a position to determine whether third-party app developers violated the Act and leaves that determination to the FTC, although we can confirm that misrepresenting the terms of an app to users is a violation of Facebook's developer policies.

Facebook has inherent incentives to protect its customers' privacy and address breaches and vulnerabilities. Indeed, the recent discovery of misconduct by an app developer on the Facebook platform clearly hurt Facebook and made it harder for us to achieve our social mission. As such, Facebook is committed to protecting our platform from bad actors, ensuring we are able to continue our mission of giving people a voice and bringing them closer together. It will take some time to work through all the changes we need to make across the company, but Facebook is committed to getting this right.

251. Does Mr. Zuckerberg support EU GDPR (General Data Protection Regulation), and should the US adopt the GDPR, would doing so negatively affect FB?

As a part of our overall approach to privacy, we are providing the same tools for access, rectification, erasure, data portability and others to people in the US (and globally) that we provide in the European Union under the GDPR. The controls and settings that Facebook is enabling as part of GDPR include settings for controlling our use of face recognition on Facebook and for controlling our ability to use data we collect off Facebook Company Products to target ads. We recently began providing direct notice of these controls and our updated terms to people around the world (including in the US), allowing people to choose whether or not to enable or disable these settings or to consent to our updated terms. Many of these tools (like our Download Your Information tool, ad preferences tool, and Activity Log) have been available globally for many years.

However, the GDPR creates some specific requirements that do not apply in the rest of the world, for example the requirement to provide contact information for the EU Data Protection Officer or to specify legal bases for processing data. We are also looking to be more responsive to regional norms and legal frameworks going forward, and want to have the flexibility to work with local regulators, which is possible with this new model. At the same time, we are changing the provisions in our Facebook, Inc. terms in our user agreements outside the United States to allow people in other countries to file lawsuits against Facebook in their home country, rather than in courts in the US. This transition was part of a continued effort to be locally responsive in countries where people use our services.

252. Should the US adopt the EU's General Data Protection Regulation (GDPR)? If not, why not?

As a part of our overall approach to privacy, we are providing the same tools for access, rectification, erasure, data portability and others to people in the US (and globally) that we provide in the European Union under the GDPR. The controls and settings that Facebook is enabling as part of GDPR include settings for controlling our use of face recognition on Facebook and for controlling our ability to use data we collect off Facebook Company Products to target ads. We recently began providing direct notice of these controls and our updated terms to people around the world (including in the US), allowing people to choose whether or not to enable or disable these settings or to consent to our updated terms. Many of these tools (like our Download Your Information tool, ad preferences tool, and Activity Log) have been available globally for many years.

However, the GDPR creates some specific requirements that do not apply in the rest of the world, for example the requirement to provide contact information for the EU Data Protection Officer or to specify legal bases for processing data. We are also looking to be more responsive to regional norms and legal frameworks going forward, and want to have the flexibility to work with local regulators, which is possible with this new model. At the same time, we are changing the provisions in our Facebook, Inc. terms in our user agreements outside the United States to allow people in other countries to file lawsuits against Facebook in their home country, rather than in courts in the US. This transition was part of a continued effort to be locally responsive in countries where people use our services.

253. Is Facebook willing to have some government regulation?

Protecting people's data is one of our most important responsibilities, and we are committed to continuing our work to improve how we protect people's information and to working with regulators to draft appropriate regulations. Our mission is to give people the power to build community and bring the world closer together. As the internet becomes more important in people's lives, the real question is about the right set of regulations that should apply to all internet services, regardless of size. Across the board, we have a responsibility to not just build tools, but to make sure that they're used in ways that are positive for our users. Facebook is generally not opposed to regulation but wants to ensure it is the right regulation. The issues facing the industry are complex, multi-faceted, and affect an important part of peoples' lives. As such, Facebook is absolutely committed to working with regulators, like Congress, to craft the right regulations.

We are already regulated in many ways—for example, under the Federal Trade Commission Act—and we are subject to ongoing oversight by the FTC under the terms of a 2011 consent order. We furnished extensive information to the FTC regarding the ability for users to port their Facebook data (including friends data that had been shared with them) with apps on Facebook's platform, as part of the FTC's investigation culminating in the July 27, 2012 Consent Order. The Consent Order memorializes the agreement between Facebook and the FTC and did not require Facebook to turn off or change the ability for people to port friends data that had been shared with them on Facebook to apps they used. Facebook voluntarily changed this feature of Platform in 2014, however. Facebook has not violated the Federal Trade Commission Act. Facebook is not in a position to determine whether third-party app developers violated the Act and leaves that determination to the FTC, although we can confirm that misrepresenting the terms of an app to users is a violation of Facebook's developer policies.

Facebook has inherent incentives to protect its customers' privacy and address breaches and vulnerabilities. Indeed, the recent discovery of misconduct by an app developer on the Facebook platform clearly hurt Facebook and made it harder for us to achieve our social mission. As such, Facebook is committed to protecting our platform from bad actors, ensuring we are able to continue our mission of giving people a voice and bringing them closer together. It will take some time to work through all the changes we need to make across the company, but Facebook is committed to getting this right.

254. **What measures ensure data breaches like this won't happen again? Can we (govt) help?**

Protecting people's data is one of our most important responsibilities, and we are committed to continuing our work to improve how we protect people's information and to working with regulators to draft appropriate regulations. Our mission is to give people the power to build community and bring the world closer together. As the internet becomes more important in people's lives, the real question is about the right set of regulations that should apply to all internet services, regardless of size. Across the board, we have a responsibility to not just build tools, but to make sure that they're used in ways that are positive for our users. Facebook is generally not opposed to regulation but wants to ensure it is the right regulation. The issues facing the industry are complex, multi-faceted, and affect an important part of peoples' lives. As such, Facebook is absolutely committed to working with regulators, like Congress, to craft the right regulations.

We are already regulated in many ways—for example, under the Federal Trade Commission Act—and we are subject to ongoing oversight by the FTC under the terms of a 2011 consent order. We furnished extensive information to the FTC regarding the ability for users to port their Facebook data (including friends data that had been shared with them) with apps on Facebook's platform, as part of the FTC's investigation culminating in the July 27, 2012 Consent Order. The Consent Order memorializes the agreement between Facebook and the FTC and did not require Facebook to turn off or change the ability for people to port friends data that had been shared with them on Facebook to apps they used. Facebook voluntarily changed this feature of Platform in 2014, however. Facebook has not violated the Federal Trade Commission Act. Facebook is not in a position to determine whether third-party app developers violated the Act and leaves that determination to the FTC, although we can confirm that misrepresenting the terms of an app to users is a violation of Facebook's developer policies.

Facebook has inherent incentives to protect its customers' privacy and address breaches and vulnerabilities. Indeed, the recent discovery of misconduct by an app developer on the Facebook platform clearly hurt Facebook and made it harder for us to achieve our social mission. As such, Facebook is committed to protecting our platform from bad actors, ensuring we are able to continue our mission of giving people a voice and bringing them closer together. It will take some time to work through all the changes we need to make across the company, but Facebook is committed to getting this right.

255. **What additional curbs should the government place on social media to prevent political hacking?**

Protecting people's data is one of our most important responsibilities, and we are committed to continuing our work to improve how we protect people's information and to working with regulators to draft appropriate regulations. Our mission is to give people the power to build community and bring the world closer together. As the internet becomes more important in people's lives, the real question is about the right set of regulations that should apply to all internet services, regardless of size. Across the board, we have a responsibility to not just build tools, but to make sure that they're used in ways that are positive for our users. Facebook is generally not opposed to regulation but wants to ensure it is the right regulation. The issues facing the industry are complex, multi-faceted, and affect an important part of peoples' lives. As such, Facebook is absolutely committed to working with regulators, like Congress, to craft the right regulations.

We are already regulated in many ways—for example, under the Federal Trade Commission Act—and we are subject to ongoing oversight by the FTC under the terms of a 2011 consent order. We furnished extensive information to the FTC regarding the ability for users to port their Facebook data (including friends data that had been shared with them) with apps on Facebook's platform, as part of the FTC's investigation culminating in the July 27, 2012 Consent Order. The Consent Order memorializes the agreement between Facebook and the FTC and did not require Facebook to turn off or change the ability for people to port friends data that had been shared with them on Facebook to apps they used. Facebook voluntarily changed this feature of Platform in 2014, however. Facebook has not violated the Federal Trade Commission Act. Facebook is not in a position to determine whether third-party app developers violated the Act

and leaves that determination to the FTC, although we can confirm that misrepresenting the terms of an app to users is a violation of Facebook's developer policies.

Facebook has inherent incentives to protect its customers' privacy and address breaches and vulnerabilities. Indeed, the recent discovery of misconduct by an app developer on the Facebook platform clearly hurt Facebook and made it harder for us to achieve our social mission. As such, Facebook is committed to protecting our platform from bad actors, ensuring we are able to continue our mission of giving people a voice and bringing them closer together. It will take some time to work through all the changes we need to make across the company, but Facebook is committed to getting this right.

256. Social media is media. Will you agree to be regulated like normal media companies are?

Protecting people's data is one of our most important responsibilities, and we are committed to continuing our work to improve how we protect people's information and to working with regulators to draft appropriate regulations. Our mission is to give people the power to build community and bring the world closer together. As the internet becomes more important in people's lives, the real question is about the right set of regulations that should apply to all internet services, regardless of size. Across the board, we have a responsibility to not just build tools, but to make sure that they're used in ways that are positive for our users. Facebook is generally not opposed to regulation but wants to ensure it is the right regulation. The issues facing the industry are complex, multi-faceted, and affect an important part of peoples' lives. As such, Facebook is absolutely committed to working with regulators, like Congress, to craft the right regulations.

We are already regulated in many ways—for example, under the Federal Trade Commission Act—and we are subject to ongoing oversight by the FTC under the terms of a 2011 consent order. We furnished extensive information to the FTC regarding the ability for users to port their Facebook data (including friends data that had been shared with them) with apps on Facebook's platform, as part of the FTC's investigation culminating in the July 27, 2012 Consent Order. The Consent Order memorializes the agreement between Facebook and the FTC and did not require Facebook to turn off or change the ability for people to port friends data that had been shared with them on Facebook to apps they used. Facebook voluntarily changed this feature of Platform in 2014, however. Facebook has not violated the Federal Trade Commission Act. Facebook is not in a position to determine whether third-party app developers violated the Act and leaves that determination to the FTC, although we can confirm that misrepresenting the terms of an app to users is a violation of Facebook's developer policies.

Facebook has inherent incentives to protect its customers' privacy and address breaches and vulnerabilities. Indeed, the recent discovery of misconduct by an app developer on the Facebook platform clearly hurt Facebook and made it harder for us to achieve our social mission. As such, Facebook is committed to protecting our platform from bad actors, ensuring we are able to continue our mission of giving people a voice and bringing them closer together. It will take some time to work through all the changes we need to make across the company, but Facebook is committed to getting this right.

257. What can our Intelligence Agencies due to better inform Facebook of likely risks and collaborate together to minimize foreign interference in our national discourse?

We want our platform to be a place where people can have authentic conversations about elections and other political topics. We believe this kind of engagement promotes democracy, but we know that there are actors working to interfere with those conversations and undermine our elections. We are already taking steps to proactively prevent election interference and we are strengthening these protections going forward.

Engagement with campaigns: We want all candidates, groups, and voters to use our platform to engage in elections. We want it to be easy for people to find, follow, and contact their elected representatives—and those running to represent them. That's why, for candidates across the political spectrum, Facebook offers the same levels of support in key moments to help campaigns understand how best to use the platform. Both the Obama and Romney campaigns had access to the same tools, and no campaign received any special treatment from Facebook. Likewise, we offered identical support to both the Trump and Clinton campaigns, and had teams assigned to both. Everyone had access to the same tools, which are the same tools that every campaign is offered, and is consistent with support provided to commercial clients in the normal course of business. Facebook representatives advise political advertisers on Facebook, as they would with other, non-political managed accounts. We have a compliance team that trains our sales representatives to comply with all federal election law requirements in this area.

While no one from Facebook was assigned full-time to the Trump campaign, Facebook employees did interact with Cambridge Analytica employees. While our investigation is ongoing, our review indicates that Facebook employees did not identify any issues involving the improper use of Facebook data in the course of their interactions with Cambridge Analytica during the 2016 US Presidential campaign.

Election Integrity: In the run-up to the 2016 elections, we were focused on the kinds of cybersecurity attacks typically used by nation states, for example phishing and malware attacks. And we were too slow to spot information operations interference. Since then, we've made important changes to prevent bad actors from using misinformation to undermine the democratic process. This will never be a solved problem because we're up against determined, creative and well-funded adversaries. But we are making steady progress. Here is a list of the 10 most important changes we have made:

- **Ads transparency.** Advertising should be transparent: users should be able to see all the ads an advertiser is currently running on Facebook, Instagram and Messenger. And for ads with political content, we've created an archive that will hold ads with political content for seven years—including information about ad impressions and spend, as well as demographic data such as age, gender and location. People in Canada and Ireland have already been able to see all the ads that a Page is running on Facebook—and we've launched this globally.

- **Verification and labeling.** Every advertiser will now need to confirm their ID and location before being able to run any ads with political content in the US. All ads with political content will also clearly state who paid for them.

- **Updating targeting.** We want ads on Facebook to be safe and civil. We thoroughly review the targeting criteria advertisers can use to ensure they are consistent with our principles. As a result, we removed nearly one-third of the targeting segments used by the IRA. We continue to allow some criteria that people may find controversial. But we do see businesses marketing things like historical books, documentaries or television shows using them in legitimate ways.

- **Better technology.** Over the past year, we've gotten increasingly better at finding and disabling fake accounts. We now block millions of fake accounts each day as people try to create them—and before they've done any harm. This is thanks to improvements in machine learning and artificial intelligence, which can proactively identify suspicious behavior at a scale that was not possible before—without needing to look at the content itself.

- **Action to tackle fake news.** We are working hard to stop the spread of false news. We work with third-party fact-checking organizations to limit the spread of articles rated false. To reduce the spread of false news, we remove fake accounts and disrupt economic incentives for traffickers of misinformation. We also use various signals, including feedback from our community, to identify potential false news. In countries where we have partnerships with independent third-party fact-checkers, stories rated as false by those fact-checkers are shown lower in News Feed. If Pages or domains repeatedly create or share misinformation, we significantly reduce their distribution and remove their advertising rights. We also want to empower people to decide for themselves what to read, trust, and share. We promote news literacy and work to inform people with more context. For example, if third-party fact-checkers write articles about a news story, we show them immediately below the story in the Related Articles unit. We also notify people and Page Admins if they try to share a story, or have shared one in the past, that's been determined to be false. In addition to our own efforts, we're learning from academics, scaling our partnerships with third-party fact-checkers and talking to other organizations about how we can work together.

  A key focus is working to disrupt the economics of fake news. For example, preventing the creation of fake accounts that spread it, banning sites that engage in this behavior from using our ad products, and demoting articles found to be false by fact checkers in News Feed—causing it to lose 80% of its traffic. We now work with independent fact checkers in the US, France, Germany, Ireland, the Netherlands, Italy, Mexico, Colombia, India, Indonesia and the Philippines with plans to scale to more countries in the coming months.

- **Significant investments in security.** We're doubling the number of people working on safety and security from 10,000 last year to over 20,000 this year. We expect these investments to impact our profitability. But the safety of people using Facebook needs to come before profit.

- **Industry collaboration.** Recently, we joined 34 global tech and security companies in signing a TechAccord pact to help improve security for everyone.

- **Information sharing and reporting channels.** In the 2017 German elections, we worked closely with the authorities there, including the Federal Office for Information Security (BSI). This gave them a dedicated reporting channel for security issues related to the federal elections.

- **Tracking 40+ elections.** In recent months, we've started to deploy new tools and teams to proactively identify threats in the run-up to specific elections. We first tested this effort during the Alabama Senate election, and plan to continue these efforts for elections around the globe, including the US midterms. Last year we used public service announcements to help inform people about fake news in 21 separate countries, including in advance of French, Kenyan and German elections.

- **Action against the Russia-based IRA.** In April, we removed 70 Facebook and 65 Instagram accounts—as well as 138 Facebook Pages—controlled by the IRA primarily targeted either at people living in Russia or Russian-speakers around the world including from neighboring countries like Azerbaijan, Uzbekistan and Ukraine. The IRA has repeatedly used complex networks of inauthentic accounts to deceive and manipulate people in the US, Europe and Russia—and we don't want them on Facebook anywhere in the world.

258. Isn't time to institute a DSGVO in the US?

As a part of our overall approach to privacy, we are providing the same tools for access, rectification, erasure, data portability and others to people in the US (and globally) that we provide in the European Union under the GDPR. The controls and settings that Facebook is enabling as part of GDPR include settings for controlling our use of face recognition on Facebook and for controlling our ability to use data we collect off Facebook Company Products to target ads. We recently began providing direct notice of these controls and our updated terms to people around the world (including in the US), allowing people to choose whether or not to enable or disable these settings or to consent to our updated terms. Many of these tools (like our Download Your Information tool, ad preferences tool, and Activity Log) have been available globally for many years.

However, the GDPR creates some specific requirements that do not apply in the rest of the world, for example the requirement to provide contact information for the EU Data Protection Officer or to specify legal bases for processing data. We are also looking to be more responsive to regional norms and legal frameworks going forward, and want to have the flexibility to work with local regulators, which is possible with this new model. At the same time, we are changing the provisions in our Facebook, Inc. terms in our user agreements outside the United States to allow people in other countries to file lawsuits against Facebook in their home country, rather than in courts in the US. This transition was part of a continued effort to be locally responsive in countries where people use our services.

259. Will Facebook agree to sufficient government oversight to insure upgraded security measures are implemented?

Protecting people's data is one of our most important responsibilities, and we are committed to continuing our work to improve how we protect people's information and to working with regulators to draft appropriate regulations. Our mission is to give people the power to build community and bring the world closer together. As the internet becomes more important in people's lives, the real question is about the right set of regulations that should apply to all internet services, regardless of size. Across the board, we have a responsibility to not just build tools, but to make sure that they're used in ways that are positive for our users. Facebook is generally not opposed to regulation but wants to ensure it is the right regulation. The issues facing the industry are complex, multi-faceted, and affect an important part of peoples' lives. As such, Facebook is absolutely committed to working with regulators, like Congress, to craft the right regulations.

We are already regulated in many ways—for example, under the Federal Trade Commission Act—and we are subject to ongoing oversight by the FTC under the terms of a 2011 consent order. We furnished extensive information to the FTC regarding the ability for users to port their Facebook data (including friends data that had been shared with them) with apps on Facebook's platform, as part of the FTC's investigation culminating in the July 27, 2012 Consent Order. The Consent Order memorializes the agreement between Facebook and the FTC and did not require Facebook to turn off or change the ability for people to port friends data that had been shared with them on Facebook to apps they used. Facebook voluntarily changed this feature of Platform in 2014, however. Facebook has not violated the Federal Trade Commission Act. Facebook is not in a position to determine whether third-party app developers violated the Act and leaves that determination to the FTC, although we can confirm that misrepresenting the terms of an app to users is a violation of Facebook's developer policies.

Facebook has inherent incentives to protect its customers' privacy and address breaches and vulnerabilities. Indeed, the recent discovery of misconduct by an app developer on the Facebook platform clearly hurt Facebook and made it harder for us to achieve our social mission. As such, Facebook is committed to protecting our platform from bad actors, ensuring we are able to continue our mission of giving people a voice and bringing them closer together. It will take some time to work through all the changes we need to make across the company, but Facebook is committed to getting this right.

260. **What public interest FCC regulation (existing or new as appropriate for your co) would you propose?**

Protecting people's data is one of our most important responsibilities, and we are committed to continuing our work to improve how we protect people's information and to working with regulators to draft appropriate regulations. Our mission is to give people the power to build community and bring the world closer together. As the internet becomes more important in people's lives, the real question is about the right set of regulations that should apply to all internet services, regardless of size. Across the board, we have a responsibility to not just build tools, but to make sure that they're used in ways that are positive for our users. Facebook is generally not opposed to regulation but wants to ensure it is the right regulation. The issues facing the industry are complex, multi-faceted, and affect an important part of peoples' lives. As such, Facebook is absolutely committed to working with regulators, like Congress, to craft the right regulations.

We are already regulated in many ways—for example, under the Federal Trade Commission Act—and we are subject to ongoing oversight by the FTC under the terms of a 2011 consent order. We furnished extensive information to the FTC regarding the ability for users to port their Facebook data (including friends data that had been shared with them) with apps on Facebook's platform, as part of the FTC's investigation culminating in the July 27, 2012 Consent Order. The Consent Order memorializes the agreement between Facebook and the FTC and did not require Facebook to turn off or change the ability for people to port friends data that had been shared with them on Facebook to apps they used. Facebook voluntarily changed this feature of Platform in 2014, however. Facebook has not violated the Federal Trade Commission Act. Facebook is not in a position to determine whether third-party app developers violated the Act and leaves that determination to the FTC, although we can confirm that misrepresenting the terms of an app to users is a violation of Facebook's developer policies.

Facebook has inherent incentives to protect its customers' privacy and address breaches and vulnerabilities. Indeed, the recent discovery of misconduct by an app developer on the Facebook platform clearly hurt Facebook and made it harder for us to achieve our social mission. As such, Facebook is committed to protecting our platform from bad actors, ensuring we are able to continue our mission of giving people a voice and bringing them closer together. It will take some time to work through all the changes we need to make across the company, but Facebook is committed to getting this right.

261. Question is for the Congress - Why don't we have data privacy laws similar to EU?

As a part of our overall approach to privacy, we are providing the same tools for access, rectification, erasure, data portability and others to people in the US (and globally) that we provide in the European Union under the GDPR. The controls and settings that Facebook is enabling as part of GDPR include settings for controlling our use of face recognition on Facebook and for controlling our ability to use data we collect off Facebook Company Products to target ads. We recently began providing direct notice of these controls and our updated terms to people around the world (including in the US), allowing people to choose whether or not to enable or disable these settings or to consent to our updated terms. Many of these tools (like our Download Your Information tool, ad preferences tool, and Activity Log) have been available globally for many years.

However, the GDPR creates some specific requirements that do not apply in the rest of the world, for example the requirement to provide contact information for the EU Data Protection Officer or to specify legal bases for processing data. We are also looking to be more responsive to regional norms and legal frameworks going forward, and want to have the flexibility to work with local regulators, which is possible with this new model. At the same time, we are changing the provisions in our Facebook, Inc. terms in our user agreements outside the United States to allow people in other countries to file lawsuits against Facebook in their home country, rather than in courts in the US. This transition was part of a continued effort to be locally responsive in countries where people use our services.

262. **Why shouldn't the United States pass personal privacy laws at least as stringent as those in Europe governing companies, including social media?**

Protecting people's data is one of our most important responsibilities, and we are committed to continuing our work to improve how we protect people's information and to working with regulators to draft appropriate regulations. Our mission is to give people the power to build community and bring the world closer together. As the internet becomes more important in people's lives, the real question is about the right set of regulations that should apply to all internet services, regardless of size. Across the board, we have a responsibility to not just build tools, but to make sure that they're used in ways that are positive for our users. Facebook is generally not opposed to regulation but wants to ensure it is the right regulation. The issues facing the industry are complex, multi-faceted, and affect an important part of peoples' lives. As such, Facebook is absolutely committed to working with regulators, like Congress, to craft the right regulations.

We are already regulated in many ways—for example, under the Federal Trade Commission Act—and we are subject to ongoing oversight by the FTC under the terms of a 2011 consent order. We furnished extensive information to the FTC regarding the ability for users to port their Facebook data (including friends data that had been shared with them) with apps on Facebook's platform, as part of the FTC's investigation culminating in the July 27, 2012 Consent Order. The Consent Order memorializes the agreement between Facebook and the FTC and did not require Facebook to turn off or change the ability for people to port friends data that had been shared with them on Facebook to apps they used. Facebook voluntarily changed this feature of Platform in 2014, however. Facebook has not violated the Federal Trade Commission Act. Facebook is not in a position to determine whether third-party app developers violated the Act and leaves that determination to the FTC, although we can confirm that misrepresenting the terms of an app to users is a violation of Facebook's developer policies.

Facebook has inherent incentives to protect its customers' privacy and address breaches and vulnerabilities. Indeed, the recent discovery of misconduct by an app developer on the Facebook platform clearly hurt Facebook and made it harder for us to achieve our social mission. As such, Facebook is committed to protecting our platform from bad actors, ensuring we are able to continue our mission of giving people a voice and bringing them closer together. It will take some time to work through all the changes we need to make across the company, but Facebook is committed to getting this right.

263. **Why should the Federal Government continue to allow Facebook to operate without placing significant restrictions to prevent future data misuse and breaches? What new actions will Facebook implement?**

Protecting people's data is one of our most important responsibilities, and we are committed to continuing our work to improve how we protect people's information and to working with regulators to draft appropriate regulations. Our mission is to give people the power to build community and bring the world closer together. As the internet becomes more important in people's lives, the real question is about the right set of regulations that should apply to all internet services, regardless of size. Across the board, we have a responsibility to not just build tools, but to make sure that they're used in ways that are positive for our users. Facebook is generally not opposed to regulation but wants to ensure it is the right regulation. The issues facing the industry are complex, multi-faceted, and affect an important part of peoples' lives. As

such, Facebook is absolutely committed to working with regulators, like Congress, to craft the right regulations.

We are already regulated in many ways—for example, under the Federal Trade Commission Act—and we are subject to ongoing oversight by the FTC under the terms of a 2011 consent order. We furnished extensive information to the FTC regarding the ability for users to port their Facebook data (including friends data that had been shared with them) with apps on Facebook's platform, as part of the FTC's investigation culminating in the July 27, 2012 Consent Order. The Consent Order memorializes the agreement between Facebook and the FTC and did not require Facebook to turn off or change the ability for people to port friends data that had been shared with them on Facebook to apps they used. Facebook voluntarily changed this feature of Platform in 2014, however. Facebook has not violated the Federal Trade Commission Act. Facebook is not in a position to determine whether third-party app developers violated the Act and leaves that determination to the FTC, although we can confirm that misrepresenting the terms of an app to users is a violation of Facebook's developer policies.

Facebook has inherent incentives to protect its customers' privacy and address breaches and vulnerabilities. Indeed, the recent discovery of misconduct by an app developer on the Facebook platform clearly hurt Facebook and made it harder for us to achieve our social mission. As such, Facebook is committed to protecting our platform from bad actors, ensuring we are able to continue our mission of giving people a voice and bringing them closer together. It will take some time to work through all the changes we need to make across the company, but Facebook is committed to getting this right.

264. What penalty should Facebook pay if it is used to unfairly influence voters in the 2018 election?

We want our platform to be a place where people can have authentic conversations about elections and other political topics. We believe this kind of engagement promotes democracy, but we know that there are actors working to interfere with those conversations and undermine our elections. We are already taking steps to proactively prevent election interference and we are strengthening these protections going forward.

Engagement with campaigns: We want all candidates, groups, and voters to use our platform to engage in elections. We want it to be easy for people to find, follow, and contact their elected representatives—and those running to represent them. That's why, for candidates across the political spectrum, Facebook offers the same levels of support in key moments to help campaigns understand how best to use the platform. Both the Obama and Romney campaigns had access to the same tools, and no campaign received any special treatment from Facebook. Likewise, we offered identical support to both the Trump and Clinton campaigns, and had teams assigned to both. Everyone had access to the same tools, which are the same tools that every campaign is offered, and is consistent with support provided to commercial clients in the normal course of business. Facebook representatives advise political advertisers on Facebook, as they would with other, non-political managed accounts. We have a compliance team that trains our sales representatives to comply with all federal election law requirements in this area.

While no one from Facebook was assigned full-time to the Trump campaign, Facebook employees did interact with Cambridge Analytica employees. While our investigation is ongoing, our review indicates that Facebook employees did not identify any issues involving the improper use of Facebook data in the course of their interactions with Cambridge Analytica during the 2016 US Presidential campaign.

Election Integrity: In the run-up to the 2016 elections, we were focused on the kinds of cybersecurity attacks typically used by nation states, for example phishing and malware attacks. And we were too slow to spot information operations interference. Since then, we've made important changes to prevent bad actors from using misinformation to undermine the democratic process. This will never be a solved problem because we're up against determined, creative and well-funded adversaries. But we are making steady progress. Here is a list of the 10 most important changes we have made:

- **Ads transparency.** Advertising should be transparent: users should be able to see all the ads an advertiser is currently running on Facebook, Instagram and Messenger. And for ads with political content, we've created an archive that will hold ads with political content for seven years—including information about ad impressions and spend, as well as demographic data such as age, gender and location. People in Canada and Ireland have already been able to see all the ads that a Page is running on Facebook—and we've launched this globally.

- **Verification and labeling.** Every advertiser will now need to confirm their ID and location before being able to run any ads with political content in the US. All ads with political content will also clearly state who paid for them.

- **Updating targeting.** We want ads on Facebook to be safe and civil. We thoroughly review the targeting criteria advertisers can use to ensure they are consistent with our principles. As a result, we removed nearly one-third of the targeting segments used by the IRA. We continue to allow some criteria that people may find controversial. But we do see businesses marketing things like historical books, documentaries or television shows using them in legitimate ways.

- **Better technology.** Over the past year, we've gotten increasingly better at finding and disabling fake accounts. We now block millions of fake accounts each day as people try to create them—and before they've done any harm. This is thanks to improvements in machine learning and artificial intelligence, which can proactively identify suspicious behavior at a scale that was not possible before—without needing to look at the content itself.

- **Action to tackle fake news.** We are working hard to stop the spread of false news. We work with third-party fact-checking organizations to limit the spread of articles rated false. To reduce the spread of false news, we remove fake accounts and disrupt economic incentives for traffickers of misinformation. We also use various signals, including feedback from our community, to identify potential false news. In countries where we have partnerships with independent third-party fact-checkers, stories rated as false by those fact-checkers are shown lower in News Feed. If Pages or domains

repeatedly create or share misinformation, we significantly reduce their distribution and remove their advertising rights. We also want to empower people to decide for themselves what to read, trust, and share. We promote news literacy and work to inform people with more context. For example, if third-party fact-checkers write articles about a news story, we show them immediately below the story in the Related Articles unit. We also notify people and Page Admins if they try to share a story, or have shared one in the past, that's been determined to be false. In addition to our own efforts, we're learning from academics, scaling our partnerships with third-party fact-checkers and talking to other organizations about how we can work together.

A key focus is working to disrupt the economics of fake news. For example, preventing the creation of fake accounts that spread it, banning sites that engage in this behavior from using our ad products, and demoting articles found to be false by fact checkers in News Feed—causing it to lose 80% of its traffic. We now work with independent fact checkers in the US, France, Germany, Ireland, the Netherlands, Italy, Mexico, Colombia, India, Indonesia and the Philippines with plans to scale to more countries in the coming months.

- **Significant investments in security.** We're doubling the number of people working on safety and security from 10,000 last year to over 20,000 this year. We expect these investments to impact our profitability. But the safety of people using Facebook needs to come before profit.

- **Industry collaboration.** Recently, we joined 34 global tech and security companies in signing a TechAccord pact to help improve security for everyone.

- **Information sharing and reporting channels.** In the 2017 German elections, we worked closely with the authorities there, including the Federal Office for Information Security (BSI). This gave them a dedicated reporting channel for security issues related to the federal elections.

- **Tracking 40+ elections.** In recent months, we've started to deploy new tools and teams to proactively identify threats in the run-up to specific elections. We first tested this effort during the Alabama Senate election, and plan to continue these efforts for elections around the globe, including the US midterms. Last year we used public service announcements to help inform people about fake news in 21 separate countries, including in advance of French, Kenyan and German elections.

- **Action against the Russia-based IRA.** In April, we removed 70 Facebook and 65 Instagram accounts—as well as 138 Facebook Pages—controlled by the IRA primarily targeted either at people living in Russia or Russian-speakers around the world including from neighboring countries like Azerbaijan, Uzbekistan and Ukraine. The IRA has repeatedly used complex networks of inauthentic accounts to deceive and manipulate people in the US, Europe and Russia—and we don't want them on Facebook anywhere in the world.

265. Hi Anna—This is a massive betrayal of every Facebook user and of democracy. Criminal negligence?

As discussed with your staff, this question is not germane to the hearing.

266. How could FB not follow up after FTC had fined them and raised concerns

Protecting people's data is one of our most important responsibilities, and we are committed to continuing our work to improve how we protect people's information and to working with regulators to draft appropriate regulations. Our mission is to give people the power to build community and bring the world closer together. As the internet becomes more important in people's lives, the real question is about the right set of regulations that should apply to all internet services, regardless of size. Across the board, we have a responsibility to not just build tools, but to make sure that they're used in ways that are positive for our users. Facebook is generally not opposed to regulation but wants to ensure it is the right regulation. The issues facing the industry are complex, multi-faceted, and affect an important part of peoples' lives. As such, Facebook is absolutely committed to working with regulators, like Congress, to craft the right regulations.

We are already regulated in many ways—for example, under the Federal Trade Commission Act—and we are subject to ongoing oversight by the FTC under the terms of a 2011 consent order. We furnished extensive information to the FTC regarding the ability for users to port their Facebook data (including friends data that had been shared with them) with apps on Facebook's platform, as part of the FTC's investigation culminating in the July 27, 2012 Consent Order. The Consent Order memorializes the agreement between Facebook and the FTC and did not require Facebook to turn off or change the ability for people to port friends data that had been shared with them on Facebook to apps they used. Facebook voluntarily changed this feature of Platform in 2014, however. Facebook has not violated the Federal Trade Commission Act. Facebook is not in a position to determine whether third-party app developers violated the Act and leaves that determination to the FTC, although we can confirm that misrepresenting the terms of an app to users is a violation of Facebook's developer policies.

Facebook has inherent incentives to protect its customers' privacy and address breaches and vulnerabilities. Indeed, the recent discovery of misconduct by an app developer on the Facebook platform clearly hurt Facebook and made it harder for us to achieve our social mission. As such, Facebook is committed to protecting our platform from bad actors, ensuring we are able to continue our mission of giving people a voice and bringing them closer together. It will take some time to work through all the changes we need to make across the company, but Facebook is committed to getting this right.

267. Mr. Zuckerberg, what do you think the US government should do to prevent abuses like this from happening again to any current, or future media system?" (Because I personally believe Facebook was, and continues to be, exploited by bad actors. Facebook SHOULD absolutely do more going forward, but we can't say they HAD to do more in the past). And I bet they know better than anyone what could be done. Hope this helps :-)

Protecting people's data is one of our most important responsibilities, and we are committed to continuing our work to improve how we protect people's information and to working with regulators to draft appropriate regulations. Our mission is to give people the power to build community and bring the world closer together. As the internet becomes more important in people's lives, the real question is about the right set of regulations that should apply to all internet services, regardless of size. Across the board, we have a responsibility to not just build tools, but to make sure that they're used in ways that are positive for our users. Facebook is generally not opposed to regulation but wants to ensure it is the right regulation. The issues facing the industry are complex, multi-faceted, and affect an important part of peoples' lives. As such, Facebook is absolutely committed to working with regulators, like Congress, to craft the right regulations.

We are already regulated in many ways—for example, under the Federal Trade Commission Act—and we are subject to ongoing oversight by the FTC under the terms of a 2011 consent order. We furnished extensive information to the FTC regarding the ability for users to port their Facebook data (including friends data that had been shared with them) with apps on Facebook's platform, as part of the FTC's investigation culminating in the July 27, 2012 Consent Order. The Consent Order memorializes the agreement between Facebook and the FTC and did not require Facebook to turn off or change the ability for people to port friends data that had been shared with them on Facebook to apps they used. Facebook voluntarily changed this feature of Platform in 2014, however. Facebook has not violated the Federal Trade Commission Act. Facebook is not in a position to determine whether third-party app developers violated the Act and leaves that determination to the FTC, although we can confirm that misrepresenting the terms of an app to users is a violation of Facebook's developer policies.

Facebook has inherent incentives to protect its customers' privacy and address breaches and vulnerabilities. Indeed, the recent discovery of misconduct by an app developer on the Facebook platform clearly hurt Facebook and made it harder for us to achieve our social mission. As such, Facebook is committed to protecting our platform from bad actors, ensuring we are able to continue our mission of giving people a voice and bringing them closer together. It will take some time to work through all the changes we need to make across the company, but Facebook is committed to getting this right.

268. What penalty is appropriate to ensure Facebook will not hide a hack again?

For years, we had been aware of other types of activity that appeared to come from Russian sources—largely traditional security threats such as attacking people's accounts or using social media platforms to spread stolen information. What we saw early in the 2016 campaign cycle followed this pattern. Our security team that focuses on threat intelligence—which investigates advanced security threats as part of our overall information security organization—was, from the outset, alert to the possibility of Russian activity. In several instances before November 8, 2016, this team detected and mitigated threats from actors with ties to Russia and reported them to US law enforcement officials. This included activity from a cluster of accounts we had assessed to belong to a group (APT28) that the US government has publicly linked to Russian military intelligence services. This activity, which was aimed at employees of major US political parties, fell into the normal categories of offensive cyber activities we monitor for. We

warned the targets who were at highest risk, and were later in contact with law enforcement authorities about this activity.

Later in the summer we also started to see a new kind of behavior from APT28-related accounts—namely, the creation of fake personas that were then used to seed stolen information to journalists. These fake personas were organized under the banner of an organization that called itself DC Leaks. This activity violated our policies, and we removed the DC Leaks accounts.

Facebook learned from press accounts and statements by congressional leaders that Russian actors might have tried to interfere in the 2016 election by exploiting Facebook's ad tools. This is not something we had seen before, and so we started an investigation. We found that fake accounts associated with the IRA tried to influence the election.

This will never be a solved problem because we're up against determined, creative and well-funded adversaries. But we are making steady progress in preventing bad actors from using misinformation to undermine the democratic process, such as: increased ad transparency, advertiser verification and labeling, updating targeting criteria, better technological efforts to find and disable fake accounts, third-party fact checking to stop the spread of false news, doubling the number of people working on safety and security, greater industry collaboration, increased information sharing and reporting channels, proactive identification of election threats, and specific action against the Russia-based IRA.

We will continue to work with the government, and across the tech industry and civil society, to address this important national security matter so that we can do our part to prevent similar abuse from happening again.

269. What level of restitution is appropriate for a data breach?

Facebook's policies regarding third-party usage of its platform technologies have prohibited—and continue to prohibit—third-party app developers from selling or licensing user data accessed from Facebook and from sharing any user data accessed from Facebook with any ad network, data broker or other advertising or monetization-related service. We take action on potential violations of our Platform Policies based on proactive review, external reports, and other signals. Kogan was not permitted to sell or transfer data to third-parties for the purposes he did. In doing so, Kogan and his company violated Facebook's Platform Policies.

On December 11, 2015, *The Guardian* published an article reporting that Kogan and his company, GSR, may have passed information the app had obtained from Facebook users to SCL Elections Ltd. (SCL)/Cambridge Analytica. Facebook immediately banned Kogan's app from our platform and investigated what happened and what further action Facebook should take to enforce our Platform Policies. Facebook considered the matter closed after obtaining written certifications and confirmations from Kogan, GSR, Cambridge Analytica, and SCL declaring that all such data they had obtained was accounted for and destroyed. We did not have any reason to affirmatively question the veracity of any of these certifications until March 2018, when we learned from media reporting that questions had been raised concerning the accuracy of the certifications. Facebook immediately banned Cambridge Analytica and SCL from purchasing

advertisements on our services as well as removed the personal accounts of some of their officers. Moreover, while Facebook's policies in place at the time allowed us to audit apps to ensure that they were safe and did not violate its terms, we had already terminated Kogan's app's access to Facebook. Accordingly, there were no ongoing concerns about the level of data that app could access or might access in the future. With the benefit of hindsight, we wish we had notified people whose information may have been impacted. Facebook has since notified all people potentially impacted with a detailed notice at the top of their News Feed.

270. Why did you ever let the Alt-Right and Neo-Nazis organize on Facebook; why do they still get to?

Freedom of expression is one of our core values, and we believe that adding voices to the conversation creates a richer and more vibrant community. We want people to feel confident that our community welcomes all viewpoints and we are committed to designing our products to give all people a voice and foster the free flow of ideas and culture. We recognize how important it is for Facebook to be a place where people feel empowered to communicate, and we take our role in keeping abuse off our service seriously. Our mission entails embracing diverse views. We err on the side of allowing content, even when some find it objectionable, unless removing that content prevents a specific harm.

However, we are, first and foremost, a technology company. Facebook does not create or edit the content that our users post on our platform. While we seek to be a platform for a broad range of ideas, we do moderate content in good faith according to published community standards in order to keep users on the platform safe, reduce objectionable content and to make sure users participate on the platform responsibly.

271. How did Donald Trump asking me to vote for him in Presidential campaign break into my FB news feed?

We want our platform to be a place where people can have authentic conversations about elections and other political topics. We believe this kind of engagement promotes democracy, but we know that there are actors working to interfere with those conversations and undermine our elections. We are already taking steps to proactively prevent election interference and we are strengthening these protections going forward.

Engagement with campaigns: We want all candidates, groups, and voters to use our platform to engage in elections. We want it to be easy for people to find, follow, and contact their elected representatives—and those running to represent them. That's why, for candidates across the political spectrum, Facebook offers the same levels of support in key moments to help campaigns understand how best to use the platform. Both the Obama and Romney campaigns had access to the same tools, and no campaign received any special treatment from Facebook. Likewise, we offered identical support to both the Trump and Clinton campaigns, and had teams assigned to both. Everyone had access to the same tools, which are the same tools that every campaign is offered, and is consistent with support provided to commercial clients in the normal course of business. Facebook representatives advise political advertisers on Facebook, as they would with other, non-political managed accounts. We have a compliance team that trains our

sales representatives to comply with all federal election law requirements in this area.

While no one from Facebook was assigned full-time to the Trump campaign, Facebook employees did interact with Cambridge Analytica employees. While our investigation is ongoing, our review indicates that Facebook employees did not identify any issues involving the improper use of Facebook data in the course of their interactions with Cambridge Analytica during the 2016 US Presidential campaign.

Election Integrity: In the run-up to the 2016 elections, we were focused on the kinds of cybersecurity attacks typically used by nation states, for example phishing and malware attacks. And we were too slow to spot information operations interference. Since then, we've made important changes to prevent bad actors from using misinformation to undermine the democratic process. This will never be a solved problem because we're up against determined, creative and well-funded adversaries. But we are making steady progress. Here is a list of the 10 most important changes we have made:

- **Ads transparency.** Advertising should be transparent: users should be able to see all the ads an advertiser is currently running on Facebook, Instagram and Messenger. And for ads with political content, we've created an archive that will hold ads with political content for seven years—including information about ad impressions and spend, as well as demographic data such as age, gender and location. People in Canada and Ireland have already been able to see all the ads that a Page is running on Facebook—and we've launched this globally.

- **Verification and labeling.** Every advertiser will now need to confirm their ID and location before being able to run any ads with political content in the US. All ads with political content will also clearly state who paid for them.

- **Updating targeting.** We want ads on Facebook to be safe and civil. We thoroughly review the targeting criteria advertisers can use to ensure they are consistent with our principles. As a result, we removed nearly one-third of the targeting segments used by the IRA. We continue to allow some criteria that people may find controversial. But we do see businesses marketing things like historical books, documentaries or television shows using them in legitimate ways.

- **Better technology.** Over the past year, we've gotten increasingly better at finding and disabling fake accounts. We now block millions of fake accounts each day as people try to create them—and before they've done any harm. This is thanks to improvements in machine learning and artificial intelligence, which can proactively identify suspicious behavior at a scale that was not possible before—without needing to look at the content itself.

- **Action to tackle fake news.** We are working hard to stop the spread of false news. We work with third-party fact-checking organizations to limit the spread of articles rated false. To reduce the spread of false news, we remove fake accounts and disrupt economic incentives for traffickers of misinformation. We also use various signals, including feedback from our community, to identify potential false news. In countries where we

have partnerships with independent third-party fact-checkers, stories rated as false by those fact-checkers are shown lower in News Feed. If Pages or domains repeatedly create or share misinformation, we significantly reduce their distribution and remove their advertising rights. We also want to empower people to decide for themselves what to read, trust, and share. We promote news literacy and work to inform people with more context. For example, if third-party fact-checkers write articles about a news story, we show them immediately below the story in the Related Articles unit. We also notify people and Page Admins if they try to share a story, or have shared one in the past, that's been determined to be false. In addition to our own efforts, we're learning from academics, scaling our partnerships with third-party fact-checkers and talking to other organizations about how we can work together.

A key focus is working to disrupt the economics of fake news. For example, preventing the creation of fake accounts that spread it, banning sites that engage in this behavior from using our ad products, and demoting articles found to be false by fact checkers in News Feed—causing it to lose 80% of its traffic. We now work with independent fact checkers in the US, France, Germany, Ireland, the Netherlands, Italy, Mexico, Colombia, India, Indonesia and the Philippines with plans to scale to more countries in the coming months.

- **Significant investments in security.** We're doubling the number of people working on safety and security from 10,000 last year to over 20,000 this year. We expect these investments to impact our profitability. But the safety of people using Facebook needs to come before profit.

- **Industry collaboration.** Recently, we joined 34 global tech and security companies in signing a TechAccord pact to help improve security for everyone.

- **Information sharing and reporting channels.** In the 2017 German elections, we worked closely with the authorities there, including the Federal Office for Information Security (BSI). This gave them a dedicated reporting channel for security issues related to the federal elections.

- **Tracking 40+ elections.** In recent months, we've started to deploy new tools and teams to proactively identify threats in the run-up to specific elections. We first tested this effort during the Alabama Senate election, and plan to continue these efforts for elections around the globe, including the US midterms. Last year we used public service announcements to help inform people about fake news in 21 separate countries, including in advance of French, Kenyan and German elections.

- **Action against the Russia-based IRA.** In April, we removed 70 Facebook and 65 Instagram accounts—as well as 138 Facebook Pages—controlled by the IRA primarily targeted either at people living in Russia or Russian-speakers around the world including from neighboring countries like Azerbaijan, Uzbekistan and Ukraine. The IRA has repeatedly used complex networks of inauthentic accounts to deceive and manipulate people in the US, Europe and Russia—and we don't want them on Facebook anywhere in the world.

272. How can you ensure that no enemies of our state—be it countries, individuals, or organizations—are paying for or otherwise proliferating political memes, ads or false news?

We want Facebook to be a place where people can discover more news, information, and perspectives, and we are working to build products that help to that. Through our News Feed algorithm, we also work hard to actively reduce the distribution of clickbait, sensationalism, and misinformation, on the one hand, and to boost news and information from sources that are trusted, informative, and local, on the other hand. We are focusing on four different strategies to address misinformation:

- **Strengthening enforcement of our authenticity policies.** We are investing heavily in new technology and hiring thousands more people to tackle the problem of inauthenticity on the platform. Fake accounts are often associated with false news, so this is an area that will have a huge impact on curbing the spread of inaccurate information.

- **Finding industry solutions.** All of us—from tech companies and media companies to newsrooms and classrooms—must work together to find industry solutions to strengthen the online news ecosystem and our own digital literacy. That's why we're collaborating with others who operate in this space. Last January, we announced The Facebook Journalism Project, an initiative that seeks to establish stronger ties between Facebook and the news industry. The project is focused on developing news products, providing training and tools for journalists, and working with publishers and educators on how we can equip people with the knowledge they need to be informed readers in the digital age. Since launching the Journalism Project, we've met with more than 2,600 publishers around the world to understand how they use our products and how we can make improvements to better support their needs.

- **Disrupting economic incentives.** When it comes to fighting false news, we've found that a lot of it is financially motivated. So, one of the most effective approaches is removing the economic incentives for those who traffic in inaccurate information. We've done things like block ads from pages that repeatedly share false news and significantly limit the distribution of web pages that deliver low quality web experiences.

- **Building new products.** We believe it's important to amplify the good effects of social media and mitigate the bad—to contribute to the diversity of ideas, information, and view points, while strengthening our common understanding.

    - We believe giving people more context can help them decide what to trust and what to share. The third-party fact-checking program we have developed uses reports from our community, along with other signals, to send stories to accredited third-party fact checking organizations. If the fact checking organizations identify a story as fake, we will suggest related articles in News Feed to show people different points of view, including information from fact checkers. Stories that have been disputed may also appear lower in News Feed. Our own data analytics show that a false rating from one of our fact checking partners reduces future impressions on Facebook by 80 percent.

- We're also testing Article Context as a way of giving people more information about the material they're reading on Facebook. Since we launched this test, some of the articles people see in News Feed will feature an "i" icon that allows them to access more information at the tap of a button. The information we surface is pulled from across the internet, and includes things like the publisher's Wikipedia entry, trending articles or related articles about the topic, and information about how the article is being shared on Facebook. In some cases, if that information is unavailable, we will let people know since that can also be helpful context.

273. What is your plan to prevent another Election 2016 disaster for the 2018 midterms?

We want our platform to be a place where people can have authentic conversations about elections and other political topics. We believe this kind of engagement promotes democracy, but we know that there are actors working to interfere with those conversations and undermine our elections. We are already taking steps to proactively prevent election interference and we are strengthening these protections going forward.

Engagement with campaigns: We want all candidates, groups, and voters to use our platform to engage in elections. We want it to be easy for people to find, follow, and contact their elected representatives—and those running to represent them. That's why, for candidates across the political spectrum, Facebook offers the same levels of support in key moments to help campaigns understand how best to use the platform. Both the Obama and Romney campaigns had access to the same tools, and no campaign received any special treatment from Facebook. Likewise, we offered identical support to both the Trump and Clinton campaigns, and had teams assigned to both. Everyone had access to the same tools, which are the same tools that every campaign is offered, and is consistent with support provided to commercial clients in the normal course of business. Facebook representatives advise political advertisers on Facebook, as they would with other, non-political managed accounts. We have a compliance team that trains our sales representatives to comply with all federal election law requirements in this area.

While no one from Facebook was assigned full-time to the Trump campaign, Facebook employees did interact with Cambridge Analytica employees. While our investigation is ongoing, our review indicates that Facebook employees did not identify any issues involving the improper use of Facebook data in the course of their interactions with Cambridge Analytica during the 2016 US Presidential campaign.

Election Integrity: In the run-up to the 2016 elections, we were focused on the kinds of cybersecurity attacks typically used by nation states, for example phishing and malware attacks. And we were too slow to spot information operations interference. Since then, we've made important changes to prevent bad actors from using misinformation to undermine the democratic process. This will never be a solved problem because we're up against determined, creative and well-funded adversaries. But we are making steady progress. Here is a list of the 10 most important changes we have made:

- **Ads transparency.** Advertising should be transparent: users should be able to see all the ads an advertiser is currently running on Facebook, Instagram and Messenger. And for ads with political content, we've created an archive that will hold ads with political

content for seven years—including information about ad impressions and spend, as well as demographic data such as age, gender and location. People in Canada and Ireland have already been able to see all the ads that a Page is running on Facebook—and we've launched this globally.

- **Verification and labeling.** Every advertiser will now need to confirm their ID and location before being able to run any ads with political content in the US. All ads with political content will also clearly state who paid for them.

- **Updating targeting.** We want ads on Facebook to be safe and civil. We thoroughly review the targeting criteria advertisers can use to ensure they are consistent with our principles. As a result, we removed nearly one-third of the targeting segments used by the IRA. We continue to allow some criteria that people may find controversial. But we do see businesses marketing things like historical books, documentaries or television shows using them in legitimate ways.

- **Better technology.** Over the past year, we've gotten increasingly better at finding and disabling fake accounts. We now block millions of fake accounts each day as people try to create them—and before they've done any harm. This is thanks to improvements in machine learning and artificial intelligence, which can proactively identify suspicious behavior at a scale that was not possible before—without needing to look at the content itself.

- **Action to tackle fake news.** We are working hard to stop the spread of false news. We work with third-party fact-checking organizations to limit the spread of articles rated false. To reduce the spread of false news, we remove fake accounts and disrupt economic incentives for traffickers of misinformation. We also use various signals, including feedback from our community, to identify potential false news. In countries where we have partnerships with independent third-party fact-checkers, stories rated as false by those fact-checkers are shown lower in News Feed. If Pages or domains repeatedly create or share misinformation, we significantly reduce their distribution and remove their advertising rights. We also want to empower people to decide for themselves what to read, trust, and share. We promote news literacy and work to inform people with more context. For example, if third-party fact-checkers write articles about a news story, we show them immediately below the story in the Related Articles unit. We also notify people and Page Admins if they try to share a story, or have shared one in the past, that's been determined to be false. In addition to our own efforts, we're learning from academics, scaling our partnerships with third-party fact-checkers and talking to other organizations about how we can work together.

  A key focus is working to disrupt the economics of fake news. For example, preventing the creation of fake accounts that spread it, banning sites that engage in this behavior from using our ad products, and demoting articles found to be false by fact checkers in News Feed—causing it to lose 80% of its traffic. We now work with independent fact checkers in the US, France, Germany, Ireland, the Netherlands, Italy, Mexico, Colombia, India, Indonesia and the Philippines with plans to scale to more countries in the coming months.

- **Significant investments in security.** We're doubling the number of people working on safety and security from 10,000 last year to over 20,000 this year. We expect these investments to impact our profitability. But the safety of people using Facebook needs to come before profit.

- **Industry collaboration.** Recently, we joined 34 global tech and security companies in signing a TechAccord pact to help improve security for everyone.

- **Information sharing and reporting channels.** In the 2017 German elections, we worked closely with the authorities there, including the Federal Office for Information Security (BSI). This gave them a dedicated reporting channel for security issues related to the federal elections.

- **Tracking 40+ elections.** In recent months, we've started to deploy new tools and teams to proactively identify threats in the run-up to specific elections. We first tested this effort during the Alabama Senate election, and plan to continue these efforts for elections around the globe, including the US midterms. Last year we used public service announcements to help inform people about fake news in 21 separate countries, including in advance of French, Kenyan and German elections.

- **Action against the Russia-based IRA.** In April, we removed 70 Facebook and 65 Instagram accounts—as well as 138 Facebook Pages—controlled by the IRA primarily targeted either at people living in Russia or Russian-speakers around the world including from neighboring countries like Azerbaijan, Uzbekistan and Ukraine. The IRA has repeatedly used complex networks of inauthentic accounts to deceive and manipulate people in the US, Europe and Russia—and we don't want them on Facebook anywhere in the world.

274. Will Facebook commit to follow the same political advertising standards print publications and broadcast networks are held to?

To build a secure product with extensive infrastructure that connects people wherever they live or whatever their income level, we need to make sure everyone can afford it. Advertising lets us keep Facebook free, which ensures it remains affordable for everyone. We also believe the ads you see across the Facebook family of apps and services should be useful and relevant to you. Users can't opt out of seeing ads altogether because selling ads is what keeps Facebook free, but they do have different options to control how their data can and can't be used to show them ads. They're all found in ad preferences, which allows users to turn off the use of all data collected from partners off Facebook to target ads. Users can also decide which of their profile fields they want used for ad targeting in the Information section under "About you." Users can remove themselves from interests under "Your interests" and categories under "Your categories." And, we do not sell people's information to anyone, and we never will.

Facebook is committed to transparency for all ads, including ads with political content. Facebook believes that people should be able to easily understand why they are seeing ads, who paid for them, and what other ads those advertisers are running. As such, Facebook only allows authorized advertisers to run ads about elections or issues that are being debated across the

country. In order to be authorized by Facebook, advertisers will need to confirm their identity and location. Furthermore, all political and issue ads will include a disclosure which reads: "Paid for by," and when users click on this disclosure they will be able to see details about the advertiser. Users will also be able to see an explanation of why they saw the particular ad. This is similar to the disclosure included on political TV advertisements. We just launched globally View Active Ads, a feature that will enable anyone to see all of the ads an advertiser is currently running by visiting the advertiser's Facebook Page.

275. What mistakes has Facebook made in handling user data & distributing false news?

We want Facebook to be a place where people can discover more news, information, and perspectives, and we are working to build products that help to that. Through our News Feed algorithm, we also work hard to actively reduce the distribution of clickbait, sensationalism, and misinformation, on the one hand, and to boost news and information from sources that are trusted, informative, and local, on the other hand. We are focusing on four different strategies to address misinformation:

- **Strengthening enforcement of our authenticity policies.** We are investing heavily in new technology and hiring thousands more people to tackle the problem of inauthenticity on the platform. Fake accounts are often associated with false news, so this is an area that will have a huge impact on curbing the spread of inaccurate information.

- **Finding industry solutions.** All of us—from tech companies and media companies to newsrooms and classrooms—must work together to find industry solutions to strengthen the online news ecosystem and our own digital literacy. That's why we're collaborating with others who operate in this space. Last January, we announced The Facebook Journalism Project, an initiative that seeks to establish stronger ties between Facebook and the news industry. The project is focused on developing news products, providing training and tools for journalists, and working with publishers and educators on how we can equip people with the knowledge they need to be informed readers in the digital age. Since launching the Journalism Project, we've met with more than 2,600 publishers around the world to understand how they use our products and how we can make improvements to better support their needs.

- **Disrupting economic incentives.** When it comes to fighting false news, we've found that a lot of it is financially motivated. So, one of the most effective approaches is removing the economic incentives for those who traffic in inaccurate information. We've done things like block ads from pages that repeatedly share false news and significantly limit the distribution of web pages that deliver low quality web experiences.

- **Building new products.** We believe it's important to amplify the good effects of social media and mitigate the bad—to contribute to the diversity of ideas, information, and view points, while strengthening our common understanding.

    - We believe giving people more context can help them decide what to trust and what to share. The third-party fact-checking program we have developed uses reports from our community, along with other signals, to send stories to

accredited third-party fact checking organizations. If the fact checking organizations identify a story as fake, we will suggest related articles in News Feed to show people different points of view, including information from fact checkers. Stories that have been disputed may also appear lower in News Feed. Our own data analytics show that a false rating from one of our fact checking partners reduces future impressions on Facebook by 80 percent.

- We're also testing Article Context as a way of giving people more information about the material they're reading on Facebook. Since we launched this test, some of the articles people see in News Feed will feature an "i" icon that allows them to access more information at the tap of a button. The information we surface is pulled from across the internet, and includes things like the publisher's Wikipedia entry, trending articles or related articles about the topic, and information about how the article is being shared on Facebook. In some cases, if that information is unavailable, we will let people know since that can also be helpful context.

276. Rather than be a force for the democratic good, Facebook is in the terrible position of supporting the rise of fascism and hatred in the US. Would Facebook be willing to start a grant program, like the one it developed for community builders, to help educate ALL American consumers about critical thinking when evaluating news, and online civility?

We want our platform to be a place where people can have authentic conversations about elections and other political topics. We believe this kind of engagement promotes democracy, but we know that there are actors working to interfere with those conversations and undermine our elections. We are already taking steps to proactively prevent election interference and we are strengthening these protections going forward.

Engagement with campaigns: We want all candidates, groups, and voters to use our platform to engage in elections. We want it to be easy for people to find, follow, and contact their elected representatives—and those running to represent them. That's why, for candidates across the political spectrum, Facebook offers the same levels of support in key moments to help campaigns understand how best to use the platform. Both the Obama and Romney campaigns had access to the same tools, and no campaign received any special treatment from Facebook. Likewise, we offered identical support to both the Trump and Clinton campaigns, and had teams assigned to both. Everyone had access to the same tools, which are the same tools that every campaign is offered, and is consistent with support provided to commercial clients in the normal course of business. Facebook representatives advise political advertisers on Facebook, as they would with other, non-political managed accounts. We have a compliance team that trains our sales representatives to comply with all federal election law requirements in this area.

While no one from Facebook was assigned full-time to the Trump campaign, Facebook employees did interact with Cambridge Analytica employees. While our investigation is ongoing, our review indicates that Facebook employees did not identify any issues involving the improper use of Facebook data in the course of their interactions with Cambridge Analytica during the 2016 US Presidential campaign.

Election Integrity: In the run-up to the 2016 elections, we were focused on the kinds of cybersecurity attacks typically used by nation states, for example phishing and malware attacks. And we were too slow to spot information operations interference. Since then, we've made important changes to prevent bad actors from using misinformation to undermine the democratic process. This will never be a solved problem because we're up against determined, creative and well-funded adversaries. But we are making steady progress. Here is a list of the 10 most important changes we have made:

- **Ads transparency.** Advertising should be transparent: users should be able to see all the ads an advertiser is currently running on Facebook, Instagram and Messenger. And for ads with political content, we've created an archive that will hold ads with political content for seven years—including information about ad impressions and spend, as well as demographic data such as age, gender and location. People in Canada and Ireland have already been able to see all the ads that a Page is running on Facebook—and we've launched this globally.

- **Verification and labeling.** Every advertiser will now need to confirm their ID and location before being able to run any ads with political content in the US. All ads with political content will also clearly state who paid for them.

- **Updating targeting.** We want ads on Facebook to be safe and civil. We thoroughly review the targeting criteria advertisers can use to ensure they are consistent with our principles. As a result, we removed nearly one-third of the targeting segments used by the IRA. We continue to allow some criteria that people may find controversial. But we do see businesses marketing things like historical books, documentaries or television shows using them in legitimate ways.

- **Better technology.** Over the past year, we've gotten increasingly better at finding and disabling fake accounts. We now block millions of fake accounts each day as people try to create them—and before they've done any harm. This is thanks to improvements in machine learning and artificial intelligence, which can proactively identify suspicious behavior at a scale that was not possible before—without needing to look at the content itself.

- **Action to tackle fake news.** We are working hard to stop the spread of false news. We work with third-party fact-checking organizations to limit the spread of articles rated false. To reduce the spread of false news, we remove fake accounts and disrupt economic incentives for traffickers of misinformation. We also use various signals, including feedback from our community, to identify potential false news. In countries where we have partnerships with independent third-party fact-checkers, stories rated as false by those fact-checkers are shown lower in News Feed. If Pages or domains repeatedly create or share misinformation, we significantly reduce their distribution and remove their advertising rights. We also want to empower people to decide for themselves what to read, trust, and share. We promote news literacy and work to inform people with more context. For example, if third-party fact-checkers write articles about a news story, we show them immediately below the story in the Related Articles unit. We also notify people and Page Admins if they try to share a story, or have shared one in the past, that's

been determined to be false. In addition to our own efforts, we're learning from academics, scaling our partnerships with third-party fact-checkers and talking to other organizations about how we can work together.

A key focus is working to disrupt the economics of fake news. For example, preventing the creation of fake accounts that spread it, banning sites that engage in this behavior from using our ad products, and demoting articles found to be false by fact checkers in News Feed—causing it to lose 80% of its traffic. We now work with independent fact checkers in the US, France, Germany, Ireland, the Netherlands, Italy, Mexico, Colombia, India, Indonesia and the Philippines with plans to scale to more countries in the coming months.

- **Significant investments in security.** We're doubling the number of people working on safety and security from 10,000 last year to over 20,000 this year. We expect these investments to impact our profitability. But the safety of people using Facebook needs to come before profit.

- **Industry collaboration.** Recently, we joined 34 global tech and security companies in signing a TechAccord pact to help improve security for everyone.

- **Information sharing and reporting channels.** In the 2017 German elections, we worked closely with the authorities there, including the Federal Office for Information Security (BSI). This gave them a dedicated reporting channel for security issues related to the federal elections.

- **Tracking 40+ elections.** In recent months, we've started to deploy new tools and teams to proactively identify threats in the run-up to specific elections. We first tested this effort during the Alabama Senate election, and plan to continue these efforts for elections around the globe, including the US midterms. Last year we used public service announcements to help inform people about fake news in 21 separate countries, including in advance of French, Kenyan and German elections.

- **Action against the Russia-based IRA.** In April, we removed 70 Facebook and 65 Instagram accounts—as well as 138 Facebook Pages—controlled by the IRA primarily targeted either at people living in Russia or Russian-speakers around the world including from neighboring countries like Azerbaijan, Uzbekistan and Ukraine. The IRA has repeatedly used complex networks of inauthentic accounts to deceive and manipulate people in the US, Europe and Russia—and we don't want them on Facebook anywhere in the world.

277. Will Facebook cooperate with the FEC to investigate allegations of collusion with political campaigns?

We want our platform to be a place where people can have authentic conversations about elections and other political topics. We believe this kind of engagement promotes democracy, but we know that there are actors working to interfere with those conversations and undermine our elections. We are already taking steps to proactively prevent election interference and we are

strengthening these protections going forward.

Engagement with campaigns: We want all candidates, groups, and voters to use our platform to engage in elections. We want it to be easy for people to find, follow, and contact their elected representatives—and those running to represent them. That's why, for candidates across the political spectrum, Facebook offers the same levels of support in key moments to help campaigns understand how best to use the platform. Both the Obama and Romney campaigns had access to the same tools, and no campaign received any special treatment from Facebook. Likewise, we offered identical support to both the Trump and Clinton campaigns, and had teams assigned to both. Everyone had access to the same tools, which are the same tools that every campaign is offered, and is consistent with support provided to commercial clients in the normal course of business. Facebook representatives advise political advertisers on Facebook, as they would with other, non-political managed accounts. We have a compliance team that trains our sales representatives to comply with all federal election law requirements in this area.

While no one from Facebook was assigned full-time to the Trump campaign, Facebook employees did interact with Cambridge Analytica employees. While our investigation is ongoing, our review indicates that Facebook employees did not identify any issues involving the improper use of Facebook data in the course of their interactions with Cambridge Analytica during the 2016 US Presidential campaign.

Election Integrity: In the run-up to the 2016 elections, we were focused on the kinds of cybersecurity attacks typically used by nation states, for example phishing and malware attacks. And we were too slow to spot information operations interference. Since then, we've made important changes to prevent bad actors from using misinformation to undermine the democratic process. This will never be a solved problem because we're up against determined, creative and well-funded adversaries. But we are making steady progress. Here is a list of the 10 most important changes we have made:

- **Ads transparency.** Advertising should be transparent: users should be able to see all the ads an advertiser is currently running on Facebook, Instagram and Messenger. And for ads with political content, we've created an archive that will hold ads with political content for seven years—including information about ad impressions and spend, as well as demographic data such as age, gender and location. People in Canada and Ireland have already been able to see all the ads that a Page is running on Facebook—and we've launched this globally.

- **Verification and labeling.** Every advertiser will now need to confirm their ID and location before being able to run any ads with political content in the US. All ads with political content will also clearly state who paid for them.

- **Updating targeting.** We want ads on Facebook to be safe and civil. We thoroughly review the targeting criteria advertisers can use to ensure they are consistent with our principles. As a result, we removed nearly one-third of the targeting segments used by the IRA. We continue to allow some criteria that people may find controversial. But we do see businesses marketing things like historical books, documentaries or television shows using them in legitimate ways.

- **Better technology.** Over the past year, we've gotten increasingly better at finding and disabling fake accounts. We now block millions of fake accounts each day as people try to create them—and before they've done any harm. This is thanks to improvements in machine learning and artificial intelligence, which can proactively identify suspicious behavior at a scale that was not possible before—without needing to look at the content itself.

- **Action to tackle fake news.** We are working hard to stop the spread of false news. We work with third-party fact-checking organizations to limit the spread of articles rated false. To reduce the spread of false news, we remove fake accounts and disrupt economic incentives for traffickers of misinformation. We also use various signals, including feedback from our community, to identify potential false news. In countries where we have partnerships with independent third-party fact-checkers, stories rated as false by those fact-checkers are shown lower in News Feed. If Pages or domains repeatedly create or share misinformation, we significantly reduce their distribution and remove their advertising rights. We also want to empower people to decide for themselves what to read, trust, and share. We promote news literacy and work to inform people with more context. For example, if third-party fact-checkers write articles about a news story, we show them immediately below the story in the Related Articles unit. We also notify people and Page Admins if they try to share a story, or have shared one in the past, that's been determined to be false. In addition to our own efforts, we're learning from academics, scaling our partnerships with third-party fact-checkers and talking to other organizations about how we can work together.

  A key focus is working to disrupt the economics of fake news. For example, preventing the creation of fake accounts that spread it, banning sites that engage in this behavior from using our ad products, and demoting articles found to be false by fact checkers in News Feed—causing it to lose 80% of its traffic. We now work with independent fact checkers in the US, France, Germany, Ireland, the Netherlands, Italy, Mexico, Colombia, India, Indonesia and the Philippines with plans to scale to more countries in the coming months.

- **Significant investments in security.** We're doubling the number of people working on safety and security from 10,000 last year to over 20,000 this year. We expect these investments to impact our profitability. But the safety of people using Facebook needs to come before profit.

- **Industry collaboration.** Recently, we joined 34 global tech and security companies in signing a TechAccord pact to help improve security for everyone.

- **Information sharing and reporting channels.** In the 2017 German elections, we worked closely with the authorities there, including the Federal Office for Information Security (BSI). This gave them a dedicated reporting channel for security issues related to the federal elections.

- **Tracking 40+ elections.** In recent months, we've started to deploy new tools and teams to proactively identify threats in the run-up to specific elections. We first tested this effort

during the Alabama Senate election, and plan to continue these efforts for elections around the globe, including the US midterms. Last year we used public service announcements to help inform people about fake news in 21 separate countries, including in advance of French, Kenyan and German elections.

- **Action against the Russia-based IRA.** In April, we removed 70 Facebook and 65 Instagram accounts—as well as 138 Facebook Pages—controlled by the IRA primarily targeted either at people living in Russia or Russian-speakers around the world including from neighboring countries like Azerbaijan, Uzbekistan and Ukraine. The IRA has repeatedly used complex networks of inauthentic accounts to deceive and manipulate people in the US, Europe and Russia—and we don't want them on Facebook anywhere in the world.

278. Did any political organization obtain personal data from Facebook prior to 2016.

We want our platform to be a place where people can have authentic conversations about elections and other political topics. We believe this kind of engagement promotes democracy, but we know that there are actors working to interfere with those conversations and undermine our elections. We are already taking steps to proactively prevent election interference and we are strengthening these protections going forward.

Engagement with campaigns: We want all candidates, groups, and voters to use our platform to engage in elections. We want it to be easy for people to find, follow, and contact their elected representatives—and those running to represent them. That's why, for candidates across the political spectrum, Facebook offers the same levels of support in key moments to help campaigns understand how best to use the platform. Both the Obama and Romney campaigns had access to the same tools, and no campaign received any special treatment from Facebook. Likewise, we offered identical support to both the Trump and Clinton campaigns, and had teams assigned to both. Everyone had access to the same tools, which are the same tools that every campaign is offered, and is consistent with support provided to commercial clients in the normal course of business. Facebook representatives advise political advertisers on Facebook, as they would with other, non-political managed accounts. We have a compliance team that trains our sales representatives to comply with all federal election law requirements in this area.

While no one from Facebook was assigned full-time to the Trump campaign, Facebook employees did interact with Cambridge Analytica employees. While our investigation is ongoing, our review indicates that Facebook employees did not identify any issues involving the improper use of Facebook data in the course of their interactions with Cambridge Analytica during the 2016 US Presidential campaign.

Election Integrity: In the run-up to the 2016 elections, we were focused on the kinds of cybersecurity attacks typically used by nation states, for example phishing and malware attacks. And we were too slow to spot information operations interference. Since then, we've made important changes to prevent bad actors from using misinformation to undermine the democratic process. This will never be a solved problem because we're up against determined, creative and well-funded adversaries. But we are making steady progress. Here is a list of the 10 most important changes we have made:

- **Ads transparency.** Advertising should be transparent: users should be able to see all the ads an advertiser is currently running on Facebook, Instagram and Messenger. And for ads with political content, we've created an archive that will hold ads with political content for seven years—including information about ad impressions and spend, as well as demographic data such as age, gender and location. People in Canada and Ireland have already been able to see all the ads that a Page is running on Facebook—and we've launched this globally.

- **Verification and labeling.** Every advertiser will now need to confirm their ID and location before being able to run any ads with political content in the US. All ads with political content will also clearly state who paid for them.

- **Updating targeting.** We want ads on Facebook to be safe and civil. We thoroughly review the targeting criteria advertisers can use to ensure they are consistent with our principles. As a result, we removed nearly one-third of the targeting segments used by the IRA. We continue to allow some criteria that people may find controversial. But we do see businesses marketing things like historical books, documentaries or television shows using them in legitimate ways.

- **Better technology.** Over the past year, we've gotten increasingly better at finding and disabling fake accounts. We now block millions of fake accounts each day as people try to create them—and before they've done any harm. This is thanks to improvements in machine learning and artificial intelligence, which can proactively identify suspicious behavior at a scale that was not possible before—without needing to look at the content itself.

- **Action to tackle fake news.** We are working hard to stop the spread of false news. We work with third-party fact-checking organizations to limit the spread of articles rated false. To reduce the spread of false news, we remove fake accounts and disrupt economic incentives for traffickers of misinformation. We also use various signals, including feedback from our community, to identify potential false news. In countries where we have partnerships with independent third-party fact-checkers, stories rated as false by those fact-checkers are shown lower in News Feed. If Pages or domains repeatedly create or share misinformation, we significantly reduce their distribution and remove their advertising rights. We also want to empower people to decide for themselves what to read, trust, and share. We promote news literacy and work to inform people with more context. For example, if third-party fact-checkers write articles about a news story, we show them immediately below the story in the Related Articles unit. We also notify people and Page Admins if they try to share a story, or have shared one in the past, that's been determined to be false. In addition to our own efforts, we're learning from academics, scaling our partnerships with third-party fact-checkers and talking to other organizations about how we can work together.

  A key focus is working to disrupt the economics of fake news. For example, preventing the creation of fake accounts that spread it, banning sites that engage in this behavior from using our ad products, and demoting articles found to be false by fact checkers in

News Feed—causing it to lose 80% of its traffic. We now work with independent fact checkers in the US, France, Germany, Ireland, the Netherlands, Italy, Mexico, Colombia, India, Indonesia and the Philippines with plans to scale to more countries in the coming months.

- **Significant investments in security.** We're doubling the number of people working on safety and security from 10,000 last year to over 20,000 this year. We expect these investments to impact our profitability. But the safety of people using Facebook needs to come before profit.

- **Industry collaboration.** Recently, we joined 34 global tech and security companies in signing a TechAccord pact to help improve security for everyone.

- **Information sharing and reporting channels.** In the 2017 German elections, we worked closely with the authorities there, including the Federal Office for Information Security (BSI). This gave them a dedicated reporting channel for security issues related to the federal elections.

- **Tracking 40+ elections.** In recent months, we've started to deploy new tools and teams to proactively identify threats in the run-up to specific elections. We first tested this effort during the Alabama Senate election, and plan to continue these efforts for elections around the globe, including the US midterms. Last year we used public service announcements to help inform people about fake news in 21 separate countries, including in advance of French, Kenyan and German elections.

- **Action against the Russia-based IRA.** In April, we removed 70 Facebook and 65 Instagram accounts—as well as 138 Facebook Pages—controlled by the IRA primarily targeted either at people living in Russia or Russian-speakers around the world including from neighboring countries like Azerbaijan, Uzbekistan and Ukraine. The IRA has repeatedly used complex networks of inauthentic accounts to deceive and manipulate people in the US, Europe and Russia—and we don't want them on Facebook anywhere in the world.

279. Ask him how it feels to be complicit in the wrongful election of Trump!!!

As discussed with your staff, this question is not germane to the hearing.

280. In hindsight, in order to avoid influencing future elections, what would you have Facebook do differently?

We want our platform to be a place where people can have authentic conversations about elections and other political topics. We believe this kind of engagement promotes democracy, but we know that there are actors working to interfere with those conversations and undermine our elections. We are already taking steps to proactively prevent election interference and we are strengthening these protections going forward.

Engagement with campaigns: We want all candidates, groups, and voters to use our platform to engage in elections. We want it to be easy for people to find, follow, and contact

their elected representatives—and those running to represent them. That's why, for candidates across the political spectrum, Facebook offers the same levels of support in key moments to help campaigns understand how best to use the platform. Both the Obama and Romney campaigns had access to the same tools, and no campaign received any special treatment from Facebook. Likewise, we offered identical support to both the Trump and Clinton campaigns, and had teams assigned to both. Everyone had access to the same tools, which are the same tools that every campaign is offered, and is consistent with support provided to commercial clients in the normal course of business. Facebook representatives advise political advertisers on Facebook, as they would with other, non-political managed accounts. We have a compliance team that trains our sales representatives to comply with all federal election law requirements in this area.

While no one from Facebook was assigned full-time to the Trump campaign, Facebook employees did interact with Cambridge Analytica employees. While our investigation is ongoing, our review indicates that Facebook employees did not identify any issues involving the improper use of Facebook data in the course of their interactions with Cambridge Analytica during the 2016 US Presidential campaign.

Election Integrity: In the run-up to the 2016 elections, we were focused on the kinds of cybersecurity attacks typically used by nation states, for example phishing and malware attacks. And we were too slow to spot information operations interference. Since then, we've made important changes to prevent bad actors from using misinformation to undermine the democratic process. This will never be a solved problem because we're up against determined, creative and well-funded adversaries. But we are making steady progress. Here is a list of the 10 most important changes we have made:

- **Ads transparency.** Advertising should be transparent: users should be able to see all the ads an advertiser is currently running on Facebook, Instagram and Messenger. And for ads with political content, we've created an archive that will hold ads with political content for seven years—including information about ad impressions and spend, as well as demographic data such as age, gender and location. People in Canada and Ireland have already been able to see all the ads that a Page is running on Facebook—and we've launched this globally.

- **Verification and labeling.** Every advertiser will now need to confirm their ID and location before being able to run any ads with political content in the US. All ads with political content will also clearly state who paid for them.

- **Updating targeting.** We want ads on Facebook to be safe and civil. We thoroughly review the targeting criteria advertisers can use to ensure they are consistent with our principles. As a result, we removed nearly one-third of the targeting segments used by the IRA. We continue to allow some criteria that people may find controversial. But we do see businesses marketing things like historical books, documentaries or television shows using them in legitimate ways.

- **Better technology.** Over the past year, we've gotten increasingly better at finding and disabling fake accounts. We now block millions of fake accounts each day as people try to create them—and before they've done any harm. This is thanks to improvements in

machine learning and artificial intelligence, which can proactively identify suspicious behavior at a scale that was not possible before—without needing to look at the content itself.

- **Action to tackle fake news.** We are working hard to stop the spread of false news. We work with third-party fact-checking organizations to limit the spread of articles rated false. To reduce the spread of false news, we remove fake accounts and disrupt economic incentives for traffickers of misinformation. We also use various signals, including feedback from our community, to identify potential false news. In countries where we have partnerships with independent third-party fact-checkers, stories rated as false by those fact-checkers are shown lower in News Feed. If Pages or domains repeatedly create or share misinformation, we significantly reduce their distribution and remove their advertising rights. We also want to empower people to decide for themselves what to read, trust, and share. We promote news literacy and work to inform people with more context. For example, if third-party fact-checkers write articles about a news story, we show them immediately below the story in the Related Articles unit. We also notify people and Page Admins if they try to share a story, or have shared one in the past, that's been determined to be false. In addition to our own efforts, we're learning from academics, scaling our partnerships with third-party fact-checkers and talking to other organizations about how we can work together.

  A key focus is working to disrupt the economics of fake news. For example, preventing the creation of fake accounts that spread it, banning sites that engage in this behavior from using our ad products, and demoting articles found to be false by fact checkers in News Feed—causing it to lose 80% of its traffic. We now work with independent fact checkers in the US, France, Germany, Ireland, the Netherlands, Italy, Mexico, Colombia, India, Indonesia and the Philippines with plans to scale to more countries in the coming months.

- **Significant investments in security.** We're doubling the number of people working on safety and security from 10,000 last year to over 20,000 this year. We expect these investments to impact our profitability. But the safety of people using Facebook needs to come before profit.

- **Industry collaboration.** Recently, we joined 34 global tech and security companies in signing a TechAccord pact to help improve security for everyone.

- **Information sharing and reporting channels.** In the 2017 German elections, we worked closely with the authorities there, including the Federal Office for Information Security (BSI). This gave them a dedicated reporting channel for security issues related to the federal elections.

- **Tracking 40+ elections.** In recent months, we've started to deploy new tools and teams to proactively identify threats in the run-up to specific elections. We first tested this effort during the Alabama Senate election, and plan to continue these efforts for elections around the globe, including the US midterms. Last year we used public service

announcements to help inform people about fake news in 21 separate countries, including in advance of French, Kenyan and German elections.

- **Action against the Russia-based IRA.** In April, we removed 70 Facebook and 65 Instagram accounts—as well as 138 Facebook Pages—controlled by the IRA primarily targeted either at people living in Russia or Russian-speakers around the world including from neighboring countries like Azerbaijan, Uzbekistan and Ukraine. The IRA has repeatedly used complex networks of inauthentic accounts to deceive and manipulate people in the US, Europe and Russia—and we don't want them on Facebook anywhere in the world.

281. Would you support impeaching Trump to atone for fake news placement and propaganda on Facebook?

As discussed with your staff, this question is not germane to the hearing.

282. Why weren't you more thoughtful about how Facebook could be leveraged by bad actors on the platform?

Facebook's policies regarding third-party usage of its platform technologies have prohibited—and continue to prohibit—third-party app developers from selling or licensing user data obtained from Facebook and from sharing any user data obtained from Facebook with any ad network, data broker or other advertising or monetization-related service.

We use a variety of tools to enforce Facebook policies against violating parties, including developers. We review tens of thousands of apps per year and regularly disapprove noncompliant apps as part of our proactive review process. We also use tools like cease and desist letters, account suspensions, letter agreements, and civil litigation. For example, since 2006, Facebook has sent over 1,150 cease-and-desist letters to over 1,600 targets. In 2017, we took action against about 370,000 apps, ranging from imposing certain restrictions to removal of the app from the platform. Moreover, we have required parties who have procured our data without authorization to delete that data. We have invested significant resources in these efforts.

Recently, we announced a number of additional steps we're taking to address concerns raised by Kogan's app.

- **Review our platform.** We will investigate all apps that had access to large amounts of data before the platform changes we announced in 2014, and we will audit any app where we identify suspicious activity. If we identify misuses of data, we'll take immediate action, including banning the app from our platform and pursuing legal action if appropriate.

- **Tell people about data misuse.** We will tell people about apps that have misused their data. This includes building a way for people to know if their data might have been accessed via the app. Moving forward, if we remove an app, we will tell people.

- **Turn off access for unused apps.** If someone has not used an app within the last three months, we will turn off the app's access to their data.

- **Restrict Facebook Login data.** We are changing Login, so that the only data that an app can request without app review will include name, profile photo, and email address. Requesting any other data will require approval from Facebook. We will also no longer allow apps to ask for access to information like religious or political views, relationship status and details, custom friends lists, education and work history, fitness activity, book reading and music listening activity, news reading, video watch activity, and games activity. We will encourage people to manage the apps they use. We already show people what apps their accounts are connected to and allow them to control what data they've permitted those apps to use. But we're making it easier for people to see what apps they use and the information they have shared with those apps.

- **Reward people who find vulnerabilities.** We launched the Data Abuse Bounty program so that people can report to us any misuses of data by app developers.

- **Update our policies.** We have updated our terms and Data Policy to explain how we use data and how data is shared with app developers.

283. Why did you collude with Russians in order to elect a madman? Ask it just like that or no vote from me.

For years, we had been aware of other types of activity that appeared to come from Russian sources—largely traditional security threats such as attacking people's accounts or using social media platforms to spread stolen information. What we saw early in the 2016 campaign cycle followed this pattern. Our security team that focuses on threat intelligence—which investigates advanced security threats as part of our overall information security organization—was, from the outset, alert to the possibility of Russian activity. In several instances before November 8, 2016, this team detected and mitigated threats from actors with ties to Russia and reported them to US law enforcement officials. This included activity from a cluster of accounts we had assessed to belong to a group (APT28) that the US government has publicly linked to Russian military intelligence services. This activity, which was aimed at employees of major US political parties, fell into the normal categories of offensive cyber activities we monitor for. We warned the targets who were at highest risk, and were later in contact with law enforcement authorities about this activity.

Later in the summer we also started to see a new kind of behavior from APT28-related accounts—namely, the creation of fake personas that were then used to seed stolen information to journalists. These fake personas were organized under the banner of an organization that called itself DC Leaks. This activity violated our policies, and we removed the DC Leaks accounts.

Facebook learned from press accounts and statements by congressional leaders that Russian actors might have tried to interfere in the 2016 election by exploiting Facebook's ad tools. This is not something we had seen before, and so we started an investigation. We found that fake accounts associated with the IRA tried to influence the election.

This will never be a solved problem because we're up against determined, creative and well-funded adversaries. But we are making steady progress in preventing bad actors from using misinformation to undermine the democratic process, such as: increased ad transparency, advertiser verification and labeling, updating targeting criteria, better technological efforts to find and disable fake accounts, third-party fact checking to stop the spread of false news, doubling the number of people working on safety and security, greater industry collaboration, increased information sharing and reporting channels, proactive identification of election threats, and specific action against the Russia-based IRA.

We will continue to work with the government, and across the tech industry and civil society, to address this important national security matter so that we can do our part to prevent similar abuse from happening again.

284. Why did FB continue to take Russian $ even though its involvement was clear months before the election.

For years, we had been aware of other types of activity that appeared to come from Russian sources—largely traditional security threats such as attacking people's accounts or using social media platforms to spread stolen information. What we saw early in the 2016 campaign cycle followed this pattern. Our security team that focuses on threat intelligence—which investigates advanced security threats as part of our overall information security organization—was, from the outset, alert to the possibility of Russian activity. In several instances before November 8, 2016, this team detected and mitigated threats from actors with ties to Russia and reported them to US law enforcement officials. This included activity from a cluster of accounts we had assessed to belong to a group (APT28) that the US government has publicly linked to Russian military intelligence services. This activity, which was aimed at employees of major US political parties, fell into the normal categories of offensive cyber activities we monitor for. We warned the targets who were at highest risk, and were later in contact with law enforcement authorities about this activity.

Later in the summer we also started to see a new kind of behavior from APT28-related accounts—namely, the creation of fake personas that were then used to seed stolen information to journalists. These fake personas were organized under the banner of an organization that called itself DC Leaks. This activity violated our policies, and we removed the DC Leaks accounts.

Facebook learned from press accounts and statements by congressional leaders that Russian actors might have tried to interfere in the 2016 election by exploiting Facebook's ad tools. This is not something we had seen before, and so we started an investigation. We found that fake accounts associated with the IRA tried to influence the election.

This will never be a solved problem because we're up against determined, creative and well-funded adversaries. But we are making steady progress in preventing bad actors from using misinformation to undermine the democratic process, such as: increased ad transparency, advertiser verification and labeling, updating targeting criteria, better technological efforts to find and disable fake accounts, third-party fact checking to stop the spread of false news, doubling the number of people working on safety and security, greater industry collaboration,

increased information sharing and reporting channels, proactive identification of election threats, and specific action against the Russia-based IRA.

We will continue to work with the government, and across the tech industry and civil society, to address this important national security matter so that we can do our part to prevent similar abuse from happening again.

285. What does Facebook plan to do to rectify the damage it has done to the 2017 Presidential election?

We want our platform to be a place where people can have authentic conversations about elections and other political topics. We believe this kind of engagement promotes democracy, but we know that there are actors working to interfere with those conversations and undermine our elections. We are already taking steps to proactively prevent election interference and we are strengthening these protections going forward.

Engagement with campaigns: We want all candidates, groups, and voters to use our platform to engage in elections. We want it to be easy for people to find, follow, and contact their elected representatives—and those running to represent them. That's why, for candidates across the political spectrum, Facebook offers the same levels of support in key moments to help campaigns understand how best to use the platform. Both the Obama and Romney campaigns had access to the same tools, and no campaign received any special treatment from Facebook. Likewise, we offered identical support to both the Trump and Clinton campaigns, and had teams assigned to both. Everyone had access to the same tools, which are the same tools that every campaign is offered, and is consistent with support provided to commercial clients in the normal course of business. Facebook representatives advise political advertisers on Facebook, as they would with other, non-political managed accounts. We have a compliance team that trains our sales representatives to comply with all federal election law requirements in this area.

While no one from Facebook was assigned full-time to the Trump campaign, Facebook employees did interact with Cambridge Analytica employees. While our investigation is ongoing, our review indicates that Facebook employees did not identify any issues involving the improper use of Facebook data in the course of their interactions with Cambridge Analytica during the 2016 US Presidential campaign.

Election Integrity: In the run-up to the 2016 elections, we were focused on the kinds of cybersecurity attacks typically used by nation states, for example phishing and malware attacks. And we were too slow to spot information operations interference. Since then, we've made important changes to prevent bad actors from using misinformation to undermine the democratic process. This will never be a solved problem because we're up against determined, creative and well-funded adversaries. But we are making steady progress. Here is a list of the 10 most important changes we have made:

- **Ads transparency.** Advertising should be transparent: users should be able to see all the ads an advertiser is currently running on Facebook, Instagram and Messenger. And for ads with political content, we've created an archive that will hold ads with political content for seven years—including information about ad impressions and spend, as well

as demographic data such as age, gender and location. People in Canada and Ireland have already been able to see all the ads that a Page is running on Facebook—and we've launched this globally.

- **Verification and labeling.** Every advertiser will now need to confirm their ID and location before being able to run any ads with political content in the US. All ads with political content will also clearly state who paid for them.

- **Updating targeting.** We want ads on Facebook to be safe and civil. We thoroughly review the targeting criteria advertisers can use to ensure they are consistent with our principles. As a result, we removed nearly one-third of the targeting segments used by the IRA. We continue to allow some criteria that people may find controversial. But we do see businesses marketing things like historical books, documentaries or television shows using them in legitimate ways.

- **Better technology.** Over the past year, we've gotten increasingly better at finding and disabling fake accounts. We now block millions of fake accounts each day as people try to create them—and before they've done any harm. This is thanks to improvements in machine learning and artificial intelligence, which can proactively identify suspicious behavior at a scale that was not possible before—without needing to look at the content itself.

- **Action to tackle fake news.** We are working hard to stop the spread of false news. We work with third-party fact-checking organizations to limit the spread of articles rated false. To reduce the spread of false news, we remove fake accounts and disrupt economic incentives for traffickers of misinformation. We also use various signals, including feedback from our community, to identify potential false news. In countries where we have partnerships with independent third-party fact-checkers, stories rated as false by those fact-checkers are shown lower in News Feed. If Pages or domains repeatedly create or share misinformation, we significantly reduce their distribution and remove their advertising rights. We also want to empower people to decide for themselves what to read, trust, and share. We promote news literacy and work to inform people with more context. For example, if third-party fact-checkers write articles about a news story, we show them immediately below the story in the Related Articles unit. We also notify people and Page Admins if they try to share a story, or have shared one in the past, that's been determined to be false. In addition to our own efforts, we're learning from academics, scaling our partnerships with third-party fact-checkers and talking to other organizations about how we can work together.

  A key focus is working to disrupt the economics of fake news. For example, preventing the creation of fake accounts that spread it, banning sites that engage in this behavior from using our ad products, and demoting articles found to be false by fact checkers in News Feed—causing it to lose 80% of its traffic. We now work with independent fact checkers in the US, France, Germany, Ireland, the Netherlands, Italy, Mexico, Colombia, India, Indonesia and the Philippines with plans to scale to more countries in the coming months.

- **Significant investments in security.** We're doubling the number of people working on safety and security from 10,000 last year to over 20,000 this year. We expect these investments to impact our profitability. But the safety of people using Facebook needs to come before profit.

- **Industry collaboration.** Recently, we joined 34 global tech and security companies in signing a TechAccord pact to help improve security for everyone.

- **Information sharing and reporting channels.** In the 2017 German elections, we worked closely with the authorities there, including the Federal Office for Information Security (BSI). This gave them a dedicated reporting channel for security issues related to the federal elections.

- **Tracking 40+ elections.** In recent months, we've started to deploy new tools and teams to proactively identify threats in the run-up to specific elections. We first tested this effort during the Alabama Senate election, and plan to continue these efforts for elections around the globe, including the US midterms. Last year we used public service announcements to help inform people about fake news in 21 separate countries, including in advance of French, Kenyan and German elections.

- **Action against the Russia-based IRA.** In April, we removed 70 Facebook and 65 Instagram accounts—as well as 138 Facebook Pages—controlled by the IRA primarily targeted either at people living in Russia or Russian-speakers around the world including from neighboring countries like Azerbaijan, Uzbekistan and Ukraine. The IRA has repeatedly used complex networks of inauthentic accounts to deceive and manipulate people in the US, Europe and Russia—and we don't want them on Facebook anywhere in the world.

286. Get out of influencing politics, both candidates and issues.

As discussed with your staff, this question is not germane to the hearing.

287. Do you feel you have a moral responsibility to ran a platform that protects our democracy?

We want our platform to be a place where people can have authentic conversations about elections and other political topics. We believe this kind of engagement promotes democracy, but we know that there are actors working to interfere with those conversations and undermine our elections. We are already taking steps to proactively prevent election interference and we are strengthening these protections going forward.

Engagement with campaigns: We want all candidates, groups, and voters to use our platform to engage in elections. We want it to be easy for people to find, follow, and contact their elected representatives—and those running to represent them. That's why, for candidates across the political spectrum, Facebook offers the same levels of support in key moments to help campaigns understand how best to use the platform. Both the Obama and Romney campaigns had access to the same tools, and no campaign received any special treatment from Facebook. Likewise, we offered identical support to both the Trump and Clinton campaigns, and had teams

assigned to both. Everyone had access to the same tools, which are the same tools that every campaign is offered, and is consistent with support provided to commercial clients in the normal course of business. Facebook representatives advise political advertisers on Facebook, as they would with other, non-political managed accounts. We have a compliance team that trains our sales representatives to comply with all federal election law requirements in this area.

While no one from Facebook was assigned full-time to the Trump campaign, Facebook employees did interact with Cambridge Analytica employees. While our investigation is ongoing, our review indicates that Facebook employees did not identify any issues involving the improper use of Facebook data in the course of their interactions with Cambridge Analytica during the 2016 US Presidential campaign.

Election Integrity: In the run-up to the 2016 elections, we were focused on the kinds of cybersecurity attacks typically used by nation states, for example phishing and malware attacks. And we were too slow to spot information operations interference. Since then, we've made important changes to prevent bad actors from using misinformation to undermine the democratic process. This will never be a solved problem because we're up against determined, creative and well-funded adversaries. But we are making steady progress. Here is a list of the 10 most important changes we have made:

- **Ads transparency.** Advertising should be transparent: users should be able to see all the ads an advertiser is currently running on Facebook, Instagram and Messenger. And for ads with political content, we've created an archive that will hold ads with political content for seven years—including information about ad impressions and spend, as well as demographic data such as age, gender and location. People in Canada and Ireland have already been able to see all the ads that a Page is running on Facebook—and we've launched this globally.

- **Verification and labeling.** Every advertiser will now need to confirm their ID and location before being able to run any ads with political content in the US. All ads with political content will also clearly state who paid for them.

- **Updating targeting.** We want ads on Facebook to be safe and civil. We thoroughly review the targeting criteria advertisers can use to ensure they are consistent with our principles. As a result, we removed nearly one-third of the targeting segments used by the IRA. We continue to allow some criteria that people may find controversial. But we do see businesses marketing things like historical books, documentaries or television shows using them in legitimate ways.

- **Better technology.** Over the past year, we've gotten increasingly better at finding and disabling fake accounts. We now block millions of fake accounts each day as people try to create them—and before they've done any harm. This is thanks to improvements in machine learning and artificial intelligence, which can proactively identify suspicious behavior at a scale that was not possible before—without needing to look at the content itself.

- **Action to tackle fake news.** We are working hard to stop the spread of false news. We work with third-party fact-checking organizations to limit the spread of articles rated false. To reduce the spread of false news, we remove fake accounts and disrupt economic incentives for traffickers of misinformation. We also use various signals, including feedback from our community, to identify potential false news. In countries where we have partnerships with independent third-party fact-checkers, stories rated as false by those fact-checkers are shown lower in News Feed. If Pages or domains repeatedly create or share misinformation, we significantly reduce their distribution and remove their advertising rights. We also want to empower people to decide for themselves what to read, trust, and share. We promote news literacy and work to inform people with more context. For example, if third-party fact-checkers write articles about a news story, we show them immediately below the story in the Related Articles unit. We also notify people and Page Admins if they try to share a story, or have shared one in the past, that's been determined to be false. In addition to our own efforts, we're learning from academics, scaling our partnerships with third-party fact-checkers and talking to other organizations about how we can work together.

  A key focus is working to disrupt the economics of fake news. For example, preventing the creation of fake accounts that spread it, banning sites that engage in this behavior from using our ad products, and demoting articles found to be false by fact checkers in News Feed—causing it to lose 80% of its traffic. We now work with independent fact checkers in the US, France, Germany, Ireland, the Netherlands, Italy, Mexico, Colombia, India, Indonesia and the Philippines with plans to scale to more countries in the coming months.

- **Significant investments in security.** We're doubling the number of people working on safety and security from 10,000 last year to over 20,000 this year. We expect these investments to impact our profitability. But the safety of people using Facebook needs to come before profit.

- **Industry collaboration.** Recently, we joined 34 global tech and security companies in signing a TechAccord pact to help improve security for everyone.

- **Information sharing and reporting channels.** In the 2017 German elections, we worked closely with the authorities there, including the Federal Office for Information Security (BSI). This gave them a dedicated reporting channel for security issues related to the federal elections.

- **Tracking 40+ elections.** In recent months, we've started to deploy new tools and teams to proactively identify threats in the run-up to specific elections. We first tested this effort during the Alabama Senate election, and plan to continue these efforts for elections around the globe, including the US midterms. Last year we used public service announcements to help inform people about fake news in 21 separate countries, including in advance of French, Kenyan and German elections.

- **Action against the Russia-based IRA.** In April, we removed 70 Facebook and 65 Instagram accounts—as well as 138 Facebook Pages—controlled by the IRA primarily

targeted either at people living in Russia or Russian-speakers around the world including from neighboring countries like Azerbaijan, Uzbekistan and Ukraine. The IRA has repeatedly used complex networks of inauthentic accounts to deceive and manipulate people in the US, Europe and Russia—and we don't want them on Facebook anywhere in the world.

288. CA bill AB 2188 would make social Media Political Ads disclose their true funders. Why not just do It?

To build a secure product with extensive infrastructure that connects people wherever they live or whatever their income level, we need to make sure everyone can afford it. Advertising lets us keep Facebook free, which ensures it remains affordable for everyone. We also believe the ads you see across the Facebook family of apps and services should be useful and relevant to you. Users can't opt out of seeing ads altogether because selling ads is what keeps Facebook free, but they do have different options to control how their data can and can't be used to show them ads. They're all found in ad preferences, which allows users to turn off the use of all data collected from partners off Facebook to target ads. Users can also decide which of their profile fields they want used for ad targeting in the Information section under "About you." Users can remove themselves from interests under "Your interests" and categories under "Your categories." And, we do not sell people's information to anyone, and we never will.

Facebook is committed to transparency for all ads, including ads with political content. Facebook believes that people should be able to easily understand why they are seeing ads, who paid for them, and what other ads those advertisers are running. As such, Facebook only allows authorized advertisers to run ads about elections or issues that are being debated across the country. In order to be authorized by Facebook, advertisers will need to confirm their identity and location. Furthermore, all political and issue ads will include a disclosure which reads: "Paid for by," and when users click on this disclosure they will be able to see details about the advertiser. Users will also be able to see an explanation of why they saw the particular ad. This is similar to the disclosure included on political TV advertisements. We just launched globally View Active Ads, a feature that will enable anyone to see all of the ads an advertiser is currently running by visiting the advertiser's Facebook Page.

289. How will you stop the divisive communications from Russia and/or other groups who strive to further their own agendas while dividing the American people?

For years, we had been aware of other types of activity that appeared to come from Russian sources—largely traditional security threats such as attacking people's accounts or using social media platforms to spread stolen information. What we saw early in the 2016 campaign cycle followed this pattern. Our security team that focuses on threat intelligence—which investigates advanced security threats as part of our overall information security organization—was, from the outset, alert to the possibility of Russian activity. In several instances before November 8, 2016, this team detected and mitigated threats from actors with ties to Russia and reported them to US law enforcement officials. This included activity from a cluster of accounts we had assessed to belong to a group (APT28) that the US government has publicly linked to Russian military intelligence services. This activity, which was aimed at employees of major US political parties, fell into the normal categories of offensive cyber activities we monitor for. We

warned the targets who were at highest risk, and were later in contact with law enforcement authorities about this activity.

Later in the summer we also started to see a new kind of behavior from APT28-related accounts—namely, the creation of fake personas that were then used to seed stolen information to journalists. These fake personas were organized under the banner of an organization that called itself DC Leaks. This activity violated our policies, and we removed the DC Leaks accounts.

Facebook learned from press accounts and statements by congressional leaders that Russian actors might have tried to interfere in the 2016 election by exploiting Facebook's ad tools. This is not something we had seen before, and so we started an investigation. We found that fake accounts associated with the IRA tried to influence the election.

This will never be a solved problem because we're up against determined, creative and well-funded adversaries. But we are making steady progress in preventing bad actors from using misinformation to undermine the democratic process, such as: increased ad transparency, advertiser verification and labeling, updating targeting criteria, better technological efforts to find and disable fake accounts, third-party fact checking to stop the spread of false news, doubling the number of people working on safety and security, greater industry collaboration, increased information sharing and reporting channels, proactive identification of election threats, and specific action against the Russia-based IRA.

We will continue to work with the government, and across the tech industry and civil society, to address this important national security matter so that we can do our part to prevent similar abuse from happening again.

290. What specifically is FB doing to stop the spread of fake news on social media?

We want Facebook to be a place where people can discover more news, information, and perspectives, and we are working to build products that help to that. Through our News Feed algorithm, we also work hard to actively reduce the distribution of clickbait, sensationalism, and misinformation, on the one hand, and to boost news and information from sources that are trusted, informative, and local, on the other hand. We are focusing on four different strategies to address misinformation:

- **Strengthening enforcement of our authenticity policies.** We are investing heavily in new technology and hiring thousands more people to tackle the problem of inauthenticity on the platform. Fake accounts are often associated with false news, so this is an area that will have a huge impact on curbing the spread of inaccurate information.

- **Finding industry solutions.** All of us—from tech companies and media companies to newsrooms and classrooms—must work together to find industry solutions to strengthen the online news ecosystem and our own digital literacy. That's why we're collaborating with others who operate in this space. Last January, we announced The Facebook Journalism Project, an initiative that seeks to establish stronger ties between Facebook and the news industry. The project is focused on developing news products, providing training and tools for journalists, and working with publishers and educators on how we

can equip people with the knowledge they need to be informed readers in the digital age. Since launching the Journalism Project, we've met with more than 2,600 publishers around the world to understand how they use our products and how we can make improvements to better support their needs.

- **Disrupting economic incentives.** When it comes to fighting false news, we've found that a lot of it is financially motivated. So, one of the most effective approaches is removing the economic incentives for those who traffic in inaccurate information. We've done things like block ads from pages that repeatedly share false news and significantly limit the distribution of web pages that deliver low quality web experiences.

- **Building new products.** We believe it's important to amplify the good effects of social media and mitigate the bad—to contribute to the diversity of ideas, information, and view points, while strengthening our common understanding.

    - We believe giving people more context can help them decide what to trust and what to share. The third-party fact-checking program we have developed uses reports from our community, along with other signals, to send stories to accredited third-party fact checking organizations. If the fact checking organizations identify a story as fake, we will suggest related articles in News Feed to show people different points of view, including information from fact checkers. Stories that have been disputed may also appear lower in News Feed. Our own data analytics show that a false rating from one of our fact checking partners reduces future impressions on Facebook by 80 percent.

    - We're also testing Article Context as a way of giving people more information about the material they're reading on Facebook. Since we launched this test, some of the articles people see in News Feed will feature an "i" icon that allows them to access more information at the tap of a button. The information we surface is pulled from across the internet, and includes things like the publisher's Wikipedia entry, trending articles or related articles about the topic, and information about how the article is being shared on Facebook. In some cases, if that information is unavailable, we will let people know since that can also be helpful context.

291. Here is another article on the two college kids who CAN figure out how to identify Russian bots. Please ask Zuckerberg why FB, with ALL their resources and smart people, can't or won't - do an even better job. Bots of ALL kinds should be clearly identified by a big red box around the post, OR better, bot accounts should be deleted entirely as soon as they are identified.
https://www.mercurynews.com/2017/11/07/as-fake-news-flies-after-the-texas-shooting-uc-berkeley-students-identify-twitter-bots-fueling-the-problem/

For years, we had been aware of other types of activity that appeared to come from Russian sources—largely traditional security threats such as attacking people's accounts or using social media platforms to spread stolen information. What we saw early in the 2016 campaign cycle followed this pattern. Our security team that focuses on threat intelligence—which investigates advanced security threats as part of our overall information security organization—

was, from the outset, alert to the possibility of Russian activity. In several instances before November 8, 2016, this team detected and mitigated threats from actors with ties to Russia and reported them to US law enforcement officials. This included activity from a cluster of accounts we had assessed to belong to a group (APT28) that the US government has publicly linked to Russian military intelligence services. This activity, which was aimed at employees of major US political parties, fell into the normal categories of offensive cyber activities we monitor for. We warned the targets who were at highest risk, and were later in contact with law enforcement authorities about this activity.

Later in the summer we also started to see a new kind of behavior from APT28-related accounts—namely, the creation of fake personas that were then used to seed stolen information to journalists. These fake personas were organized under the banner of an organization that called itself DC Leaks. This activity violated our policies, and we removed the DC Leaks accounts.

Facebook learned from press accounts and statements by congressional leaders that Russian actors might have tried to interfere in the 2016 election by exploiting Facebook's ad tools. This is not something we had seen before, and so we started an investigation. We found that fake accounts associated with the IRA tried to influence the election.

This will never be a solved problem because we're up against determined, creative and well-funded adversaries. But we are making steady progress in preventing bad actors from using misinformation to undermine the democratic process, such as: increased ad transparency, advertiser verification and labeling, updating targeting criteria, better technological efforts to find and disable fake accounts, third-party fact checking to stop the spread of false news, doubling the number of people working on safety and security, greater industry collaboration, increased information sharing and reporting channels, proactive identification of election threats, and specific action against the Russia-based IRA.

We will continue to work with the government, and across the tech industry and civil society, to address this important national security matter so that we can do our part to prevent similar abuse from happening again.

292. What went wrong that enabled these bad actors to manipulate Facebook to influence the American electorate? What specific policies and protections can we put in place to make sure that this never happens again? Doe can that be enforced without getting government into your (and others) technical processes? If you were a govt administrator responsible to insure that Russian and other foreign bad actors couldn't access Americans private information and manipulate Americans as they did with Facebook in 2018, what would you do?

For years, we had been aware of other types of activity that appeared to come from Russian sources—largely traditional security threats such as attacking people's accounts or using social media platforms to spread stolen information. What we saw early in the 2016 campaign cycle followed this pattern. Our security team that focuses on threat intelligence—which investigates advanced security threats as part of our overall information security organization—was, from the outset, alert to the possibility of Russian activity. In several instances before

November 8, 2016, this team detected and mitigated threats from actors with ties to Russia and reported them to US law enforcement officials. This included activity from a cluster of accounts we had assessed to belong to a group (APT28) that the US government has publicly linked to Russian military intelligence services. This activity, which was aimed at employees of major US political parties, fell into the normal categories of offensive cyber activities we monitor for. We warned the targets who were at highest risk, and were later in contact with law enforcement authorities about this activity.

Later in the summer we also started to see a new kind of behavior from APT28-related accounts—namely, the creation of fake personas that were then used to seed stolen information to journalists. These fake personas were organized under the banner of an organization that called itself DC Leaks. This activity violated our policies, and we removed the DC Leaks accounts.

Facebook learned from press accounts and statements by congressional leaders that Russian actors might have tried to interfere in the 2016 election by exploiting Facebook's ad tools. This is not something we had seen before, and so we started an investigation. We found that fake accounts associated with the IRA tried to influence the election.

This will never be a solved problem because we're up against determined, creative and well-funded adversaries. But we are making steady progress in preventing bad actors from using misinformation to undermine the democratic process, such as: increased ad transparency, advertiser verification and labeling, updating targeting criteria, better technological efforts to find and disable fake accounts, third-party fact checking to stop the spread of false news, doubling the number of people working on safety and security, greater industry collaboration, increased information sharing and reporting channels, proactive identification of election threats, and specific action against the Russia-based IRA.

We will continue to work with the government, and across the tech industry and civil society, to address this important national security matter so that we can do our part to prevent similar abuse from happening again.

293. What do you plan to do to address the spread of fake news and propaganda which your platform facilitates? Why were you so dismissive about the usage of FB to disseminate lies and hatred when concerns were raised by your employees before the presidential election?

We want Facebook to be a place where people can discover more news, information, and perspectives, and we are working to build products that help to that. Through our News Feed algorithm, we also work hard to actively reduce the distribution of clickbait, sensationalism, and misinformation, on the one hand, and to boost news and information from sources that are trusted, informative, and local, on the other hand.

We are focusing on four different strategies to address misinformation:

- **Strengthening enforcement of our authenticity policies.** We are investing heavily in new technology and hiring thousands more people to tackle the problem of inauthenticity

on the platform. Fake accounts are often associated with false news, so this is an area that will have a huge impact on curbing the spread of inaccurate information.

- **Finding industry solutions.** All of us—from tech companies and media companies to newsrooms and classrooms—must work together to find industry solutions to strengthen the online news ecosystem and our own digital literacy. That's why we're collaborating with others who operate in this space. Last January, we announced The Facebook Journalism Project, an initiative that seeks to establish stronger ties between Facebook and the news industry. The project is focused on developing news products, providing training and tools for journalists, and working with publishers and educators on how we can equip people with the knowledge they need to be informed readers in the digital age. Since launching the Journalism Project, we've met with more than 2,600 publishers around the world to understand how they use our products and how we can make improvements to better support their needs.

- **Disrupting economic incentives.** When it comes to fighting false news, we've found that a lot of it is financially motivated. So, one of the most effective approaches is removing the economic incentives for those who traffic in inaccurate information. We've done things like block ads from pages that repeatedly share false news and significantly limit the distribution of web pages that deliver low quality web experiences.

- **Building new products.** We believe it's important to amplify the good effects of social media and mitigate the bad—to contribute to the diversity of ideas, information, and view points, while strengthening our common understanding.

    - We believe giving people more context can help them decide what to trust and what to share. The third-party fact-checking program we have developed uses reports from our community, along with other signals, to send stories to accredited third-party fact checking organizations. If the fact checking organizations identify a story as fake, we will suggest related articles in News Feed to show people different points of view, including information from fact checkers. Stories that have been disputed may also appear lower in News Feed. Our own data analytics show that a false rating from one of our fact checking partners reduces future impressions on Facebook by 80 percent.

    - We're also testing Article Context as a way of giving people more information about the material they're reading on Facebook. Since we launched this test, some of the articles people see in News Feed will feature an "i" icon that allows them to access more information at the tap of a button. The information we surface is pulled from across the internet, and includes things like the publisher's Wikipedia entry, trending articles or related articles about the topic, and information about how the article is being shared on Facebook. In some cases, if that information is unavailable, we will let people know since that can also be helpful context.

294. Is your plan to stay politically globally neutral or is it to favor a position by featuring one and obscuring another?

Freedom of expression is one of our core values, and we believe that adding voices to the conversation creates a richer and more vibrant community. We want people to feel confident that our community welcomes all viewpoints and we are committed to designing our products to give all people a voice and foster the free flow of ideas and culture. We recognize how important it is for Facebook to be a place where people feel empowered to communicate, and we take our role in keeping abuse off our service seriously. Our mission entails embracing diverse views. We err on the side of allowing content, even when some find it objectionable, unless removing that content prevents a specific harm.

However, we are, first and foremost, a technology company. Facebook does not create or edit the content that our users post on our platform. While we seek to be a platform for a broad range of ideas, we do moderate content in good faith according to published community standards in order to keep users on the platform safe, reduce objectionable content and to make sure users participate on the platform responsibly.

295. Does Facebook have a responsibility to promote democracy? If so, how can you implement this?

We want our platform to be a place where people can have authentic conversations about elections and other political topics. We believe this kind of engagement promotes democracy, but we know that there are actors working to interfere with those conversations and undermine our elections. We are already taking steps to proactively prevent election interference and we are strengthening these protections going forward.

Engagement with campaigns: We want all candidates, groups, and voters to use our platform to engage in elections. We want it to be easy for people to find, follow, and contact their elected representatives—and those running to represent them. That's why, for candidates across the political spectrum, Facebook offers the same levels of support in key moments to help campaigns understand how best to use the platform. Both the Obama and Romney campaigns had access to the same tools, and no campaign received any special treatment from Facebook. Likewise, we offered identical support to both the Trump and Clinton campaigns, and had teams assigned to both. Everyone had access to the same tools, which are the same tools that every campaign is offered, and is consistent with support provided to commercial clients in the normal course of business. Facebook representatives advise political advertisers on Facebook, as they would with other, non-political managed accounts. We have a compliance team that trains our sales representatives to comply with all federal election law requirements in this area.

While no one from Facebook was assigned full-time to the Trump campaign, Facebook employees did interact with Cambridge Analytica employees. While our investigation is ongoing, our review indicates that Facebook employees did not identify any issues involving the improper use of Facebook data in the course of their interactions with Cambridge Analytica during the 2016 US Presidential campaign.

Election Integrity: In the run-up to the 2016 elections, we were focused on the kinds of cybersecurity attacks typically used by nation states, for example phishing and malware attacks. And we were too slow to spot information operations interference. Since then, we've made important changes to prevent bad actors from using misinformation to undermine the democratic

process. This will never be a solved problem because we're up against determined, creative and well-funded adversaries. But we are making steady progress. Here is a list of the 10 most important changes we have made:

- **Ads transparency.** Advertising should be transparent: users should be able to see all the ads an advertiser is currently running on Facebook, Instagram and Messenger. And for ads with political content, we've created an archive that will hold ads with political content for seven years—including information about ad impressions and spend, as well as demographic data such as age, gender and location. People in Canada and Ireland have already been able to see all the ads that a Page is running on Facebook—and we've launched this globally.

- **Verification and labeling.** Every advertiser will now need to confirm their ID and location before being able to run any ads with political content in the US. All ads with political content will also clearly state who paid for them.

- **Updating targeting.** We want ads on Facebook to be safe and civil. We thoroughly review the targeting criteria advertisers can use to ensure they are consistent with our principles. As a result, we removed nearly one-third of the targeting segments used by the IRA. We continue to allow some criteria that people may find controversial. But we do see businesses marketing things like historical books, documentaries or television shows using them in legitimate ways.

- **Better technology.** Over the past year, we've gotten increasingly better at finding and disabling fake accounts. We now block millions of fake accounts each day as people try to create them—and before they've done any harm. This is thanks to improvements in machine learning and artificial intelligence, which can proactively identify suspicious behavior at a scale that was not possible before—without needing to look at the content itself.

- **Action to tackle fake news.** We are working hard to stop the spread of false news. We work with third-party fact-checking organizations to limit the spread of articles rated false. To reduce the spread of false news, we remove fake accounts and disrupt economic incentives for traffickers of misinformation. We also use various signals, including feedback from our community, to identify potential false news. In countries where we have partnerships with independent third-party fact-checkers, stories rated as false by those fact-checkers are shown lower in News Feed. If Pages or domains repeatedly create or share misinformation, we significantly reduce their distribution and remove their advertising rights. We also want to empower people to decide for themselves what to read, trust, and share. We promote news literacy and work to inform people with more context. For example, if third-party fact-checkers write articles about a news story, we show them immediately below the story in the Related Articles unit. We also notify people and Page Admins if they try to share a story, or have shared one in the past, that's been determined to be false. In addition to our own efforts, we're learning from academics, scaling our partnerships with third-party fact-checkers and talking to other organizations about how we can work together.

A key focus is working to disrupt the economics of fake news. For example, preventing the creation of fake accounts that spread it, banning sites that engage in this behavior from using our ad products, and demoting articles found to be false by fact checkers in News Feed—causing it to lose 80% of its traffic. We now work with independent fact checkers in the US, France, Germany, Ireland, the Netherlands, Italy, Mexico, Colombia, India, Indonesia and the Philippines with plans to scale to more countries in the coming months.

- **Significant investments in security.** We're doubling the number of people working on safety and security from 10,000 last year to over 20,000 this year. We expect these investments to impact our profitability. But the safety of people using Facebook needs to come before profit.

- **Industry collaboration.** Recently, we joined 34 global tech and security companies in signing a TechAccord pact to help improve security for everyone.

- **Information sharing and reporting channels.** In the 2017 German elections, we worked closely with the authorities there, including the Federal Office for Information Security (BSI). This gave them a dedicated reporting channel for security issues related to the federal elections.

- **Tracking 40+ elections.** In recent months, we've started to deploy new tools and teams to proactively identify threats in the run-up to specific elections. We first tested this effort during the Alabama Senate election, and plan to continue these efforts for elections around the globe, including the US midterms. Last year we used public service announcements to help inform people about fake news in 21 separate countries, including in advance of French, Kenyan and German elections.

- **Action against the Russia-based IRA.** In April, we removed 70 Facebook and 65 Instagram accounts—as well as 138 Facebook Pages—controlled by the IRA primarily targeted either at people living in Russia or Russian-speakers around the world including from neighboring countries like Azerbaijan, Uzbekistan and Ukraine. The IRA has repeatedly used complex networks of inauthentic accounts to deceive and manipulate people in the US, Europe and Russia—and we don't want them on Facebook anywhere in the world.

296. The most primitive "big data" analysis tool would have discovered the foreign influence. Why was it not used?

For years, we had been aware of other types of activity that appeared to come from Russian sources—largely traditional security threats such as attacking people's accounts or using social media platforms to spread stolen information. What we saw early in the 2016 campaign cycle followed this pattern. Our security team that focuses on threat intelligence—which investigates advanced security threats as part of our overall information security organization—was, from the outset, alert to the possibility of Russian activity. In several instances before November 8, 2016, this team detected and mitigated threats from actors with ties to Russia and reported them to US law enforcement officials. This included activity from a cluster of accounts

we had assessed to belong to a group (APT28) that the US government has publicly linked to Russian military intelligence services. This activity, which was aimed at employees of major US political parties, fell into the normal categories of offensive cyber activities we monitor for. We warned the targets who were at highest risk, and were later in contact with law enforcement authorities about this activity.

Later in the summer we also started to see a new kind of behavior from APT28-related accounts—namely, the creation of fake personas that were then used to seed stolen information to journalists. These fake personas were organized under the banner of an organization that called itself DC Leaks. This activity violated our policies, and we removed the DC Leaks accounts.

Facebook learned from press accounts and statements by congressional leaders that Russian actors might have tried to interfere in the 2016 election by exploiting Facebook's ad tools. This is not something we had seen before, and so we started an investigation. We found that fake accounts associated with the IRA tried to influence the election.

This will never be a solved problem because we're up against determined, creative and well-funded adversaries. But we are making steady progress in preventing bad actors from using misinformation to undermine the democratic process, such as: increased ad transparency, advertiser verification and labeling, updating targeting criteria, better technological efforts to find and disable fake accounts, third-party fact checking to stop the spread of false news, doubling the number of people working on safety and security, greater industry collaboration, increased information sharing and reporting channels, proactive identification of election threats, and specific action against the Russia-based IRA.

We will continue to work with the government, and across the tech industry and civil society, to address this important national security matter so that we can do our part to prevent similar abuse from happening again.

297. Why is Andrew Bosworth still working at Facebook after encouraging both the Russian influence ad campaign, and, the Cambridge Analytica breach with his disturbing growth memo? Why did you then say that he has a divergent viewpoint last month and acknowledge its authenticity and seriousness, while exposing your failed obligation to enforce ethics with your executives as CEO and Chairman of the Board? Mr. Bosworth wouldn't be employed elsewhere making such statements...I want to know how you feel you can be effective as Facebooks CEO and chairman now?

We recognize that we have made mistakes, and we are committed to learning from this experience to secure our platform further and make our community safer for everyone going forward. As our CEO Mark Zuckerberg has said, when you are building something unprecedented like Facebook, there are going to be mistakes. What people should hold us accountable for is learning from the mistakes and continually doing better—and, at the end of the day, making sure that we're building things that people like and that make their lives better.

Particularly in the past few months, we've realized that we need to take a broader view of our responsibility to our community. Part of that effort is continuing our ongoing efforts to identify ways that we can improve our privacy practices. We've heard loud and clear that privacy settings and other important tools are too hard to find and that we must do more to keep people informed. So, we're taking additional steps to put people more in control of their privacy. For instance, we redesigned our entire settings menu on mobile devices from top to bottom to make things easier to find. We also created a new Privacy Shortcuts in a menu where users can control their data in just a few taps, with clearer explanations of how our controls work. The experience is now clearer, more visual, and easy-to-find. Furthermore, we also updated our terms of service that include our commitments to everyone using Facebook. We explain the services we offer in language that's easier to read. We've also updated our Data Policy to better spell out what data we collect and how we use it in Facebook, Instagram, Messenger, and other products.

298. Were there earlier incidents of malicious third parties in prior elections, and if so, why were they undisclosed?

We want our platform to be a place where people can have authentic conversations about elections and other political topics. We believe this kind of engagement promotes democracy, but we know that there are actors working to interfere with those conversations and undermine our elections. We are already taking steps to proactively prevent election interference and we are strengthening these protections going forward.

Engagement with campaigns: We want all candidates, groups, and voters to use our platform to engage in elections. We want it to be easy for people to find, follow, and contact their elected representatives—and those running to represent them. That's why, for candidates across the political spectrum, Facebook offers the same levels of support in key moments to help campaigns understand how best to use the platform. Both the Obama and Romney campaigns had access to the same tools, and no campaign received any special treatment from Facebook. Likewise, we offered identical support to both the Trump and Clinton campaigns, and had teams assigned to both. Everyone had access to the same tools, which are the same tools that every campaign is offered, and is consistent with support provided to commercial clients in the normal course of business. Facebook representatives advise political advertisers on Facebook, as they would with other, non-political managed accounts. We have a compliance team that trains our sales representatives to comply with all federal election law requirements in this area.

While no one from Facebook was assigned full-time to the Trump campaign, Facebook employees did interact with Cambridge Analytica employees. While our investigation is ongoing, our review indicates that Facebook employees did not identify any issues involving the improper use of Facebook data in the course of their interactions with Cambridge Analytica during the 2016 US Presidential campaign.

Election Integrity: In the run-up to the 2016 elections, we were focused on the kinds of cybersecurity attacks typically used by nation states, for example phishing and malware attacks. And we were too slow to spot information operations interference. Since then, we've made important changes to prevent bad actors from using misinformation to undermine the democratic process. This will never be a solved problem because we're up against determined, creative and

well-funded adversaries. But we are making steady progress. Here is a list of the 10 most important changes we have made:

- **Ads transparency.** Advertising should be transparent: users should be able to see all the ads an advertiser is currently running on Facebook, Instagram and Messenger. And for ads with political content, we've created an archive that will hold ads with political content for seven years—including information about ad impressions and spend, as well as demographic data such as age, gender and location. People in Canada and Ireland have already been able to see all the ads that a Page is running on Facebook—and we've launched this globally.

- **Verification and labeling.** Every advertiser will now need to confirm their ID and location before being able to run any ads with political content in the US. All ads with political content will also clearly state who paid for them.

- **Updating targeting.** We want ads on Facebook to be safe and civil. We thoroughly review the targeting criteria advertisers can use to ensure they are consistent with our principles. As a result, we removed nearly one-third of the targeting segments used by the IRA. We continue to allow some criteria that people may find controversial. But we do see businesses marketing things like historical books, documentaries or television shows using them in legitimate ways.

- **Better technology.** Over the past year, we've gotten increasingly better at finding and disabling fake accounts. We now block millions of fake accounts each day as people try to create them—and before they've done any harm. This is thanks to improvements in machine learning and artificial intelligence, which can proactively identify suspicious behavior at a scale that was not possible before—without needing to look at the content itself.

- **Action to tackle fake news.** We are working hard to stop the spread of false news. We work with third-party fact-checking organizations to limit the spread of articles rated false. To reduce the spread of false news, we remove fake accounts and disrupt economic incentives for traffickers of misinformation. We also use various signals, including feedback from our community, to identify potential false news. In countries where we have partnerships with independent third-party fact-checkers, stories rated as false by those fact-checkers are shown lower in News Feed. If Pages or domains repeatedly create or share misinformation, we significantly reduce their distribution and remove their advertising rights. We also want to empower people to decide for themselves what to read, trust, and share. We promote news literacy and work to inform people with more context. For example, if third-party fact-checkers write articles about a news story, we show them immediately below the story in the Related Articles unit. We also notify people and Page Admins if they try to share a story, or have shared one in the past, that's been determined to be false. In addition to our own efforts, we're learning from academics, scaling our partnerships with third-party fact-checkers and talking to other organizations about how we can work together.

  A key focus is working to disrupt the economics of fake news. For example, preventing

the creation of fake accounts that spread it, banning sites that engage in this behavior from using our ad products, and demoting articles found to be false by fact checkers in News Feed—causing it to lose 80% of its traffic. We now work with independent fact checkers in the US, France, Germany, Ireland, the Netherlands, Italy, Mexico, Colombia, India, Indonesia and the Philippines with plans to scale to more countries in the coming months.

- **Significant investments in security.** We're doubling the number of people working on safety and security from 10,000 last year to over 20,000 this year. We expect these investments to impact our profitability. But the safety of people using Facebook needs to come before profit.

- **Industry collaboration.** Recently, we joined 34 global tech and security companies in signing a TechAccord pact to help improve security for everyone.

- **Information sharing and reporting channels.** In the 2017 German elections, we worked closely with the authorities there, including the Federal Office for Information Security (BSI). This gave them a dedicated reporting channel for security issues related to the federal elections.

- **Tracking 40+ elections.** In recent months, we've started to deploy new tools and teams to proactively identify threats in the run-up to specific elections. We first tested this effort during the Alabama Senate election, and plan to continue these efforts for elections around the globe, including the US midterms. Last year we used public service announcements to help inform people about fake news in 21 separate countries, including in advance of French, Kenyan and German elections.

- **Action against the Russia-based IRA.** In April, we removed 70 Facebook and 65 Instagram accounts—as well as 138 Facebook Pages—controlled by the IRA primarily targeted either at people living in Russia or Russian-speakers around the world including from neighboring countries like Azerbaijan, Uzbekistan and Ukraine. The IRA has repeatedly used complex networks of inauthentic accounts to deceive and manipulate people in the US, Europe and Russia—and we don't want them on Facebook anywhere in the world.

299. When was Facebook First aware that user data may have been compromised for political purposes?

We want our platform to be a place where people can have authentic conversations about elections and other political topics. We believe this kind of engagement promotes democracy, but we know that there are actors working to interfere with those conversations and undermine our elections. We are already taking steps to proactively prevent election interference and we are strengthening these protections going forward.

Engagement with campaigns: We want all candidates, groups, and voters to use our platform to engage in elections. We want it to be easy for people to find, follow, and contact their elected representatives—and those running to represent them. That's why, for candidates

across the political spectrum, Facebook offers the same levels of support in key moments to help campaigns understand how best to use the platform. Both the Obama and Romney campaigns had access to the same tools, and no campaign received any special treatment from Facebook. Likewise, we offered identical support to both the Trump and Clinton campaigns, and had teams assigned to both. Everyone had access to the same tools, which are the same tools that every campaign is offered, and is consistent with support provided to commercial clients in the normal course of business. Facebook representatives advise political advertisers on Facebook, as they would with other, non-political managed accounts. We have a compliance team that trains our sales representatives to comply with all federal election law requirements in this area.

While no one from Facebook was assigned full-time to the Trump campaign, Facebook employees did interact with Cambridge Analytica employees. While our investigation is ongoing, our review indicates that Facebook employees did not identify any issues involving the improper use of Facebook data in the course of their interactions with Cambridge Analytica during the 2016 US Presidential campaign.

Election Integrity: In the run-up to the 2016 elections, we were focused on the kinds of cybersecurity attacks typically used by nation states, for example phishing and malware attacks. And we were too slow to spot information operations interference. Since then, we've made important changes to prevent bad actors from using misinformation to undermine the democratic process. This will never be a solved problem because we're up against determined, creative and well-funded adversaries. But we are making steady progress. Here is a list of the 10 most important changes we have made:

- **Ads transparency.** Advertising should be transparent: users should be able to see all the ads an advertiser is currently running on Facebook, Instagram and Messenger. And for ads with political content, we've created an archive that will hold ads with political content for seven years—including information about ad impressions and spend, as well as demographic data such as age, gender and location. People in Canada and Ireland have already been able to see all the ads that a Page is running on Facebook—and we've launched this globally.

- **Verification and labeling.** Every advertiser will now need to confirm their ID and location before being able to run any ads with political content in the US. All ads with political content will also clearly state who paid for them.

- **Updating targeting.** We want ads on Facebook to be safe and civil. We thoroughly review the targeting criteria advertisers can use to ensure they are consistent with our principles. As a result, we removed nearly one-third of the targeting segments used by the IRA. We continue to allow some criteria that people may find controversial. But we do see businesses marketing things like historical books, documentaries or television shows using them in legitimate ways.

- **Better technology.** Over the past year, we've gotten increasingly better at finding and disabling fake accounts. We now block millions of fake accounts each day as people try to create them—and before they've done any harm. This is thanks to improvements in machine learning and artificial intelligence, which can proactively identify suspicious

behavior at a scale that was not possible before—without needing to look at the content itself.

- **Action to tackle fake news.** We are working hard to stop the spread of false news. We work with third-party fact-checking organizations to limit the spread of articles rated false. To reduce the spread of false news, we remove fake accounts and disrupt economic incentives for traffickers of misinformation. We also use various signals, including feedback from our community, to identify potential false news. In countries where we have partnerships with independent third-party fact-checkers, stories rated as false by those fact-checkers are shown lower in News Feed. If Pages or domains repeatedly create or share misinformation, we significantly reduce their distribution and remove their advertising rights. We also want to empower people to decide for themselves what to read, trust, and share. We promote news literacy and work to inform people with more context. For example, if third-party fact-checkers write articles about a news story, we show them immediately below the story in the Related Articles unit. We also notify people and Page Admins if they try to share a story, or have shared one in the past, that's been determined to be false. In addition to our own efforts, we're learning from academics, scaling our partnerships with third-party fact-checkers and talking to other organizations about how we can work together.

  A key focus is working to disrupt the economics of fake news. For example, preventing the creation of fake accounts that spread it, banning sites that engage in this behavior from using our ad products, and demoting articles found to be false by fact checkers in News Feed—causing it to lose 80% of its traffic. We now work with independent fact checkers in the US, France, Germany, Ireland, the Netherlands, Italy, Mexico, Colombia, India, Indonesia and the Philippines with plans to scale to more countries in the coming months.

- **Significant investments in security.** We're doubling the number of people working on safety and security from 10,000 last year to over 20,000 this year. We expect these investments to impact our profitability. But the safety of people using Facebook needs to come before profit.

- **Industry collaboration.** Recently, we joined 34 global tech and security companies in signing a TechAccord pact to help improve security for everyone.

- **Information sharing and reporting channels.** In the 2017 German elections, we worked closely with the authorities there, including the Federal Office for Information Security (BSI). This gave them a dedicated reporting channel for security issues related to the federal elections.

- **Tracking 40+ elections.** In recent months, we've started to deploy new tools and teams to proactively identify threats in the run-up to specific elections. We first tested this effort during the Alabama Senate election, and plan to continue these efforts for elections around the globe, including the US midterms. Last year we used public service announcements to help inform people about fake news in 21 separate countries, including in advance of French, Kenyan and German elections.

- **Action against the Russia-based IRA.** In April, we removed 70 Facebook and 65 Instagram accounts—as well as 138 Facebook Pages—controlled by the IRA primarily targeted either at people living in Russia or Russian-speakers around the world including from neighboring countries like Azerbaijan, Uzbekistan and Ukraine. The IRA has repeatedly used complex networks of inauthentic accounts to deceive and manipulate people in the US, Europe and Russia—and we don't want them on Facebook anywhere in the world.

300. How you will block fake and doctored videos from your users' uploads?

We want Facebook to be a place where people can discover more news, information, and perspectives, and we are working to build products that help to that. Through our News Feed algorithm, we also work hard to actively reduce the distribution of clickbait, sensationalism, and misinformation, on the one hand, and to boost news and information from sources that are trusted, informative, and local, on the other hand.

We are focusing on four different strategies to address misinformation:

- **Strengthening enforcement of our authenticity policies.** We are investing heavily in new technology and hiring thousands more people to tackle the problem of inauthenticity on the platform. Fake accounts are often associated with false news, so this is an area that will have a huge impact on curbing the spread of inaccurate information.

- **Finding industry solutions.** All of us—from tech companies and media companies to newsrooms and classrooms—must work together to find industry solutions to strengthen the online news ecosystem and our own digital literacy. That's why we're collaborating with others who operate in this space. Last January, we announced The Facebook Journalism Project, an initiative that seeks to establish stronger ties between Facebook and the news industry. The project is focused on developing news products, providing training and tools for journalists, and working with publishers and educators on how we can equip people with the knowledge they need to be informed readers in the digital age. Since launching the Journalism Project, we've met with more than 2,600 publishers around the world to understand how they use our products and how we can make improvements to better support their needs.

- **Disrupting economic incentives.** When it comes to fighting false news, we've found that a lot of it is financially motivated. So, one of the most effective approaches is removing the economic incentives for those who traffic in inaccurate information. We've done things like block ads from pages that repeatedly share false news and significantly limit the distribution of web pages that deliver low quality web experiences.

- **Building new products.** We believe it's important to amplify the good effects of social media and mitigate the bad—to contribute to the diversity of ideas, information, and view points, while strengthening our common understanding.

    - We believe giving people more context can help them decide what to trust and what to share. The third-party fact-checking program we have developed uses reports from our community, along with other signals, to send stories to

accredited third-party fact checking organizations. If the fact checking organizations identify a story as fake, we will suggest related articles in News Feed to show people different points of view, including information from fact checkers. Stories that have been disputed may also appear lower in News Feed. Our own data analytics show that a false rating from one of our fact checking partners reduces future impressions on Facebook by 80 percent.

- We're also testing Article Context as a way of giving people more information about the material they're reading on Facebook. Since we launched this test, some of the articles people see in News Feed will feature an "i" icon that allows them to access more information at the tap of a button. The information we surface is pulled from across the internet, and includes things like the publisher's Wikipedia entry, trending articles or related articles about the topic, and information about how the article is being shared on Facebook. In some cases, if that information is unavailable, we will let people know since that can also be helpful context.

301. What bad actors have my profile and personal profile photo? I want a list so I can defend myself.

Facebook's policies regarding third-party usage of its platform technologies have prohibited—and continue to prohibit—third-party app developers from selling or licensing user data obtained from Facebook and from sharing any user data obtained from Facebook with any ad network, data broker or other advertising or monetization-related service.

We use a variety of tools to enforce Facebook policies against violating parties, including developers. We review tens of thousands of apps per year and regularly disapprove noncompliant apps as part of our proactive review process. We also use tools like cease and desist letters, account suspensions, letter agreements, and civil litigation. For example, since 2006, Facebook has sent over 1,150 cease-and-desist letters to over 1,600 targets. In 2017, we took action against about 370,000 apps, ranging from imposing certain restrictions to removal of the app from the platform. Moreover, we have required parties who have procured our data without authorization to delete that data. We have invested significant resources in these efforts.

Recently, we announced a number of additional steps we're taking to address concerns raised by Kogan's app.

- **Review our platform.** We will investigate all apps that had access to large amounts of data before the platform changes we announced in 2014, and we will audit any app where we identify suspicious activity. If we identify misuses of data, we'll take immediate action, including banning the app from our platform and pursuing legal action if appropriate.

- **Tell people about data misuse.** We will tell people about apps that have misused their data. This includes building a way for people to know if their data might have been accessed via the app. Moving forward, if we remove an app, we will tell people.

- **Turn off access for unused apps.** If someone has not used an app within the last three months, we will turn off the app's access to their data.

- **Restrict Facebook Login data.** We are changing Login, so that the only data that an app can request without app review will include name, profile photo, and email address. Requesting any other data will require approval from Facebook. We will also no longer allow apps to ask for access to information like religious or political views, relationship status and details, custom friends lists, education and work history, fitness activity, book reading and music listening activity, news reading, video watch activity, and games activity. We will encourage people to manage the apps they use. We already show people what apps their accounts are connected to and allow them to control what data they've permitted those apps to use. But we're making it easier for people to see what apps they use and the information they have shared with those apps.

- **Reward people who find vulnerabilities.** We launched the Data Abuse Bounty program so that people can report to us any misuses of data by app developers.

- **Update our policies.** We have updated our terms and Data Policy to explain how we use data and how data is shared with app developers.

302. How will you verify users in the future to make sure that those communicating on Facebook are real?

Claiming to be another person violates our Community Standards, and we want to make it harder for anyone to be impersonated on our platform, as well as more effectively detect and deactivate fake accounts to help reduce the spread of spam, false news, and misinformation.

We continually update our technical systems to identify, checkpoint, and remove inauthentic accounts, and we block millions of attempts to register fake accounts every day. As with all security threats, we have been incorporating new insights into our models for detecting fake accounts, including information specific to election issues. We've developed several techniques to help detect and block this type of abuse. At the time someone receives a friend request, our systems are designed to check whether the recipient already has a friend with the same name, along with a variety of other factors that help us determine if an interaction is legitimate. Further, we recently announced new features that use face recognition technology that may help detect when someone is using another user's image as their profile photo—which helps stop impersonation. Users can also report accounts that are impersonating them. This is an area we're continually working to improve so that we can provide a safe and secure experience on Facebook.

303. To what extent do you feel responsible for the corruption of reality the right wing is suffering?

We want our platform to be a place where people can have authentic conversations about elections and other political topics. We believe this kind of engagement promotes democracy, but we know that there are actors working to interfere with those conversations and undermine our elections. We are already taking steps to proactively prevent election interference and we are

strengthening these protections going forward.

Engagement with campaigns: We want all candidates, groups, and voters to use our platform to engage in elections. We want it to be easy for people to find, follow, and contact their elected representatives—and those running to represent them. That's why, for candidates across the political spectrum, Facebook offers the same levels of support in key moments to help campaigns understand how best to use the platform. Both the Obama and Romney campaigns had access to the same tools, and no campaign received any special treatment from Facebook. Likewise, we offered identical support to both the Trump and Clinton campaigns, and had teams assigned to both. Everyone had access to the same tools, which are the same tools that every campaign is offered, and is consistent with support provided to commercial clients in the normal course of business. Facebook representatives advise political advertisers on Facebook, as they would with other, non-political managed accounts. We have a compliance team that trains our sales representatives to comply with all federal election law requirements in this area.

While no one from Facebook was assigned full-time to the Trump campaign, Facebook employees did interact with Cambridge Analytica employees. While our investigation is ongoing, our review indicates that Facebook employees did not identify any issues involving the improper use of Facebook data in the course of their interactions with Cambridge Analytica during the 2016 US Presidential campaign.

Election Integrity: In the run-up to the 2016 elections, we were focused on the kinds of cybersecurity attacks typically used by nation states, for example phishing and malware attacks. And we were too slow to spot information operations interference. Since then, we've made important changes to prevent bad actors from using misinformation to undermine the democratic process. This will never be a solved problem because we're up against determined, creative and well-funded adversaries. But we are making steady progress. Here is a list of the 10 most important changes we have made:

- **Ads transparency.** Advertising should be transparent: users should be able to see all the ads an advertiser is currently running on Facebook, Instagram and Messenger. And for ads with political content, we've created an archive that will hold ads with political content for seven years—including information about ad impressions and spend, as well as demographic data such as age, gender and location. People in Canada and Ireland have already been able to see all the ads that a Page is running on Facebook—and we've launched this globally.

- **Verification and labeling.** Every advertiser will now need to confirm their ID and location before being able to run any ads with political content in the US. All ads with political content will also clearly state who paid for them.

- **Updating targeting.** We want ads on Facebook to be safe and civil. We thoroughly review the targeting criteria advertisers can use to ensure they are consistent with our principles. As a result, we removed nearly one-third of the targeting segments used by the IRA. We continue to allow some criteria that people may find controversial. But we do see businesses marketing things like historical books, documentaries or television shows using them in legitimate ways.

- **Better technology.** Over the past year, we've gotten increasingly better at finding and disabling fake accounts. We now block millions of fake accounts each day as people try to create them—and before they've done any harm. This is thanks to improvements in machine learning and artificial intelligence, which can proactively identify suspicious behavior at a scale that was not possible before—without needing to look at the content itself.

- **Action to tackle fake news.** We are working hard to stop the spread of false news. We work with third-party fact-checking organizations to limit the spread of articles rated false. To reduce the spread of false news, we remove fake accounts and disrupt economic incentives for traffickers of misinformation. We also use various signals, including feedback from our community, to identify potential false news. In countries where we have partnerships with independent third-party fact-checkers, stories rated as false by those fact-checkers are shown lower in News Feed. If Pages or domains repeatedly create or share misinformation, we significantly reduce their distribution and remove their advertising rights. We also want to empower people to decide for themselves what to read, trust, and share. We promote news literacy and work to inform people with more context. For example, if third-party fact-checkers write articles about a news story, we show them immediately below the story in the Related Articles unit. We also notify people and Page Admins if they try to share a story, or have shared one in the past, that's been determined to be false. In addition to our own efforts, we're learning from academics, scaling our partnerships with third-party fact-checkers and talking to other organizations about how we can work together.

  A key focus is working to disrupt the economics of fake news. For example, preventing the creation of fake accounts that spread it, banning sites that engage in this behavior from using our ad products, and demoting articles found to be false by fact checkers in News Feed—causing it to lose 80% of its traffic. We now work with independent fact checkers in the US, France, Germany, Ireland, the Netherlands, Italy, Mexico, Colombia, India, Indonesia and the Philippines with plans to scale to more countries in the coming months.

- **Significant investments in security.** We're doubling the number of people working on safety and security from 10,000 last year to over 20,000 this year. We expect these investments to impact our profitability. But the safety of people using Facebook needs to come before profit.

- **Industry collaboration.** Recently, we joined 34 global tech and security companies in signing a TechAccord pact to help improve security for everyone.

- **Information sharing and reporting channels.** In the 2017 German elections, we worked closely with the authorities there, including the Federal Office for Information Security (BSI). This gave them a dedicated reporting channel for security issues related to the federal elections.

- **Tracking 40+ elections.** In recent months, we've started to deploy new tools and teams to proactively identify threats in the run-up to specific elections. We first tested this effort

during the Alabama Senate election, and plan to continue these efforts for elections around the globe, including the US midterms. Last year we used public service announcements to help inform people about fake news in 21 separate countries, including in advance of French, Kenyan and German elections.

- **Action against the Russia-based IRA.** In April, we removed 70 Facebook and 65 Instagram accounts—as well as 138 Facebook Pages—controlled by the IRA primarily targeted either at people living in Russia or Russian-speakers around the world including from neighboring countries like Azerbaijan, Uzbekistan and Ukraine. The IRA has repeatedly used complex networks of inauthentic accounts to deceive and manipulate people in the US, Europe and Russia—and we don't want them on Facebook anywhere in the world.

304. What fraction of Facebook's income comes from the sale of people's data, from the dissemination of questionable information and from the sale of advertisements to external political organizations such as Russia? Would it hurt Facebook so much as to eliminate these sources of income?

For years, we had been aware of other types of activity that appeared to come from Russian sources—largely traditional security threats such as attacking people's accounts or using social media platforms to spread stolen information. What we saw early in the 2016 campaign cycle followed this pattern. Our security team that focuses on threat intelligence—which investigates advanced security threats as part of our overall information security organization—was, from the outset, alert to the possibility of Russian activity. In several instances before November 8, 2016, this team detected and mitigated threats from actors with ties to Russia and reported them to US law enforcement officials. This included activity from a cluster of accounts we had assessed to belong to a group (APT28) that the US government has publicly linked to Russian military intelligence services. This activity, which was aimed at employees of major US political parties, fell into the normal categories of offensive cyber activities we monitor for. We warned the targets who were at highest risk, and were later in contact with law enforcement authorities about this activity.

Later in the summer we also started to see a new kind of behavior from APT28-related accounts—namely, the creation of fake personas that were then used to seed stolen information to journalists. These fake personas were organized under the banner of an organization that called itself DC Leaks. This activity violated our policies, and we removed the DC Leaks accounts.

Facebook learned from press accounts and statements by congressional leaders that Russian actors might have tried to interfere in the 2016 election by exploiting Facebook's ad tools. This is not something we had seen before, and so we started an investigation. We found that fake accounts associated with the IRA tried to influence the election.

This will never be a solved problem because we're up against determined, creative and well-funded adversaries. But we are making steady progress in preventing bad actors from using misinformation to undermine the democratic process, such as: increased ad transparency, advertiser verification and labeling, updating targeting criteria, better technological efforts to

find and disable fake accounts, third-party fact checking to stop the spread of false news, doubling the number of people working on safety and security, greater industry collaboration, increased information sharing and reporting channels, proactive identification of election threats, and specific action against the Russia-based IRA.

We will continue to work with the government, and across the tech industry and civil society, to address this important national security matter so that we can do our part to prevent similar abuse from happening again.

305. Could Facebook construct and maintain social network graphs of cyber propaganda sites on Facebook?

We want our platform to be a place where people can have authentic conversations about elections and other political topics. We believe this kind of engagement promotes democracy, but we know that there are actors working to interfere with those conversations and undermine our elections. We are already taking steps to proactively prevent election interference and we are strengthening these protections going forward.

Engagement with campaigns: We want all candidates, groups, and voters to use our platform to engage in elections. We want it to be easy for people to find, follow, and contact their elected representatives—and those running to represent them. That's why, for candidates across the political spectrum, Facebook offers the same levels of support in key moments to help campaigns understand how best to use the platform. Both the Obama and Romney campaigns had access to the same tools, and no campaign received any special treatment from Facebook. Likewise, we offered identical support to both the Trump and Clinton campaigns, and had teams assigned to both. Everyone had access to the same tools, which are the same tools that every campaign is offered, and is consistent with support provided to commercial clients in the normal course of business. Facebook representatives advise political advertisers on Facebook, as they would with other, non-political managed accounts. We have a compliance team that trains our sales representatives to comply with all federal election law requirements in this area.

While no one from Facebook was assigned full-time to the Trump campaign, Facebook employees did interact with Cambridge Analytica employees. While our investigation is ongoing, our review indicates that Facebook employees did not identify any issues involving the improper use of Facebook data in the course of their interactions with Cambridge Analytica during the 2016 US Presidential campaign.

Election Integrity: In the run-up to the 2016 elections, we were focused on the kinds of cybersecurity attacks typically used by nation states, for example phishing and malware attacks. And we were too slow to spot information operations interference. Since then, we've made important changes to prevent bad actors from using misinformation to undermine the democratic process. This will never be a solved problem because we're up against determined, creative and well-funded adversaries. But we are making steady progress. Here is a list of the 10 most important changes we have made:

- **Ads transparency.** Advertising should be transparent: users should be able to see all the ads an advertiser is currently running on Facebook, Instagram and Messenger. And for

ads with political content, we've created an archive that will hold ads with political content for seven years—including information about ad impressions and spend, as well as demographic data such as age, gender and location. People in Canada and Ireland have already been able to see all the ads that a Page is running on Facebook—and we've launched this globally.

- **Verification and labeling.** Every advertiser will now need to confirm their ID and location before being able to run any ads with political content in the US. All ads with political content will also clearly state who paid for them.

- **Updating targeting.** We want ads on Facebook to be safe and civil. We thoroughly review the targeting criteria advertisers can use to ensure they are consistent with our principles. As a result, we removed nearly one-third of the targeting segments used by the IRA. We continue to allow some criteria that people may find controversial. But we do see businesses marketing things like historical books, documentaries or television shows using them in legitimate ways.

- **Better technology.** Over the past year, we've gotten increasingly better at finding and disabling fake accounts. We now block millions of fake accounts each day as people try to create them—and before they've done any harm. This is thanks to improvements in machine learning and artificial intelligence, which can proactively identify suspicious behavior at a scale that was not possible before—without needing to look at the content itself.

- **Action to tackle fake news.** We are working hard to stop the spread of false news. We work with third-party fact-checking organizations to limit the spread of articles rated false. To reduce the spread of false news, we remove fake accounts and disrupt economic incentives for traffickers of misinformation. We also use various signals, including feedback from our community, to identify potential false news. In countries where we have partnerships with independent third-party fact-checkers, stories rated as false by those fact-checkers are shown lower in News Feed. If Pages or domains repeatedly create or share misinformation, we significantly reduce their distribution and remove their advertising rights. We also want to empower people to decide for themselves what to read, trust, and share. We promote news literacy and work to inform people with more context. For example, if third-party fact-checkers write articles about a news story, we show them immediately below the story in the Related Articles unit. We also notify people and Page Admins if they try to share a story, or have shared one in the past, that's been determined to be false. In addition to our own efforts, we're learning from academics, scaling our partnerships with third-party fact-checkers and talking to other organizations about how we can work together.

  A key focus is working to disrupt the economics of fake news. For example, preventing the creation of fake accounts that spread it, banning sites that engage in this behavior from using our ad products, and demoting articles found to be false by fact checkers in News Feed—causing it to lose 80% of its traffic. We now work with independent fact checkers in the US, France, Germany, Ireland, the Netherlands, Italy, Mexico, Colombia,

India, Indonesia and the Philippines with plans to scale to more countries in the coming months.

- **Significant investments in security.** We're doubling the number of people working on safety and security from 10,000 last year to over 20,000 this year. We expect these investments to impact our profitability. But the safety of people using Facebook needs to come before profit.

- **Industry collaboration.** Recently, we joined 34 global tech and security companies in signing a TechAccord pact to help improve security for everyone.

- **Information sharing and reporting channels.** In the 2017 German elections, we worked closely with the authorities there, including the Federal Office for Information Security (BSI). This gave them a dedicated reporting channel for security issues related to the federal elections.

- **Tracking 40+ elections.** In recent months, we've started to deploy new tools and teams to proactively identify threats in the run-up to specific elections. We first tested this effort during the Alabama Senate election, and plan to continue these efforts for elections around the globe, including the US midterms. Last year we used public service announcements to help inform people about fake news in 21 separate countries, including in advance of French, Kenyan and German elections.

- **Action against the Russia-based IRA.** In April, we removed 70 Facebook and 65 Instagram accounts—as well as 138 Facebook Pages—controlled by the IRA primarily targeted either at people living in Russia or Russian-speakers around the world including from neighboring countries like Azerbaijan, Uzbekistan and Ukraine. The IRA has repeatedly used complex networks of inauthentic accounts to deceive and manipulate people in the US, Europe and Russia—and we don't want them on Facebook anywhere in the world.

306. How could your company accept money on political posts and not think it was against our Constitution.

We want our platform to be a place where people can have authentic conversations about elections and other political topics. We believe this kind of engagement promotes democracy, but we know that there are actors working to interfere with those conversations and undermine our elections. We are already taking steps to proactively prevent election interference and we are strengthening these protections going forward.

Engagement with campaigns: We want all candidates, groups, and voters to use our platform to engage in elections. We want it to be easy for people to find, follow, and contact their elected representatives—and those running to represent them. That's why, for candidates across the political spectrum, Facebook offers the same levels of support in key moments to help campaigns understand how best to use the platform. Both the Obama and Romney campaigns had access to the same tools, and no campaign received any special treatment from Facebook. Likewise, we offered identical support to both the Trump and Clinton campaigns, and had teams

assigned to both. Everyone had access to the same tools, which are the same tools that every campaign is offered, and is consistent with support provided to commercial clients in the normal course of business. Facebook representatives advise political advertisers on Facebook, as they would with other, non-political managed accounts. We have a compliance team that trains our sales representatives to comply with all federal election law requirements in this area.

While no one from Facebook was assigned full-time to the Trump campaign, Facebook employees did interact with Cambridge Analytica employees. While our investigation is ongoing, our review indicates that Facebook employees did not identify any issues involving the improper use of Facebook data in the course of their interactions with Cambridge Analytica during the 2016 US Presidential campaign.

Election Integrity: In the run-up to the 2016 elections, we were focused on the kinds of cybersecurity attacks typically used by nation states, for example phishing and malware attacks. And we were too slow to spot information operations interference. Since then, we've made important changes to prevent bad actors from using misinformation to undermine the democratic process. This will never be a solved problem because we're up against determined, creative and well-funded adversaries. But we are making steady progress. Here is a list of the 10 most important changes we have made:

- **Ads transparency.** Advertising should be transparent: users should be able to see all the ads an advertiser is currently running on Facebook, Instagram and Messenger. And for ads with political content, we've created an archive that will hold ads with political content for seven years—including information about ad impressions and spend, as well as demographic data such as age, gender and location. People in Canada and Ireland have already been able to see all the ads that a Page is running on Facebook—and we've launched this globally.

- **Verification and labeling.** Every advertiser will now need to confirm their ID and location before being able to run any ads with political content in the US. All ads with political content will also clearly state who paid for them.

- **Updating targeting.** We want ads on Facebook to be safe and civil. We thoroughly review the targeting criteria advertisers can use to ensure they are consistent with our principles. As a result, we removed nearly one-third of the targeting segments used by the IRA. We continue to allow some criteria that people may find controversial. But we do see businesses marketing things like historical books, documentaries or television shows using them in legitimate ways.

- **Better technology.** Over the past year, we've gotten increasingly better at finding and disabling fake accounts. We now block millions of fake accounts each day as people try to create them—and before they've done any harm. This is thanks to improvements in machine learning and artificial intelligence, which can proactively identify suspicious behavior at a scale that was not possible before—without needing to look at the content itself.

- **Action to tackle fake news.** We are working hard to stop the spread of false news. We work with third-party fact-checking organizations to limit the spread of articles rated false. To reduce the spread of false news, we remove fake accounts and disrupt economic incentives for traffickers of misinformation. We also use various signals, including feedback from our community, to identify potential false news. In countries where we have partnerships with independent third-party fact-checkers, stories rated as false by those fact-checkers are shown lower in News Feed. If Pages or domains repeatedly create or share misinformation, we significantly reduce their distribution and remove their advertising rights. We also want to empower people to decide for themselves what to read, trust, and share. We promote news literacy and work to inform people with more context. For example, if third-party fact-checkers write articles about a news story, we show them immediately below the story in the Related Articles unit. We also notify people and Page Admins if they try to share a story, or have shared one in the past, that's been determined to be false. In addition to our own efforts, we're learning from academics, scaling our partnerships with third-party fact-checkers and talking to other organizations about how we can work together.

  A key focus is working to disrupt the economics of fake news. For example, preventing the creation of fake accounts that spread it, banning sites that engage in this behavior from using our ad products, and demoting articles found to be false by fact checkers in News Feed—causing it to lose 80% of its traffic. We now work with independent fact checkers in the US, France, Germany, Ireland, the Netherlands, Italy, Mexico, Colombia, India, Indonesia and the Philippines with plans to scale to more countries in the coming months.

- **Significant investments in security.** We're doubling the number of people working on safety and security from 10,000 last year to over 20,000 this year. We expect these investments to impact our profitability. But the safety of people using Facebook needs to come before profit.

- **Industry collaboration.** Recently, we joined 34 global tech and security companies in signing a TechAccord pact to help improve security for everyone.

- **Information sharing and reporting channels.** In the 2017 German elections, we worked closely with the authorities there, including the Federal Office for Information Security (BSI). This gave them a dedicated reporting channel for security issues related to the federal elections.

- **Tracking 40+ elections.** In recent months, we've started to deploy new tools and teams to proactively identify threats in the run-up to specific elections. We first tested this effort during the Alabama Senate election, and plan to continue these efforts for elections around the globe, including the US midterms. Last year we used public service announcements to help inform people about fake news in 21 separate countries, including in advance of French, Kenyan and German elections.

- **Action against the Russia-based IRA.** In April, we removed 70 Facebook and 65 Instagram accounts—as well as 138 Facebook Pages—controlled by the IRA primarily

targeted either at people living in Russia or Russian-speakers around the world including from neighboring countries like Azerbaijan, Uzbekistan and Ukraine. The IRA has repeatedly used complex networks of inauthentic accounts to deceive and manipulate people in the US, Europe and Russia—and we don't want them on Facebook anywhere in the world.

307. How will you prevent Facebook from thwarting our elections?

We want our platform to be a place where people can have authentic conversations about elections and other political topics. We believe this kind of engagement promotes democracy, but we know that there are actors working to interfere with those conversations and undermine our elections. We are already taking steps to proactively prevent election interference and we are strengthening these protections going forward.

Engagement with campaigns: We want all candidates, groups, and voters to use our platform to engage in elections. We want it to be easy for people to find, follow, and contact their elected representatives—and those running to represent them. That's why, for candidates across the political spectrum, Facebook offers the same levels of support in key moments to help campaigns understand how best to use the platform. Both the Obama and Romney campaigns had access to the same tools, and no campaign received any special treatment from Facebook. Likewise, we offered identical support to both the Trump and Clinton campaigns, and had teams assigned to both. Everyone had access to the same tools, which are the same tools that every campaign is offered, and is consistent with support provided to commercial clients in the normal course of business. Facebook representatives advise political advertisers on Facebook, as they would with other, non-political managed accounts. We have a compliance team that trains our sales representatives to comply with all federal election law requirements in this area.

While no one from Facebook was assigned full-time to the Trump campaign, Facebook employees did interact with Cambridge Analytica employees. While our investigation is ongoing, our review indicates that Facebook employees did not identify any issues involving the improper use of Facebook data in the course of their interactions with Cambridge Analytica during the 2016 US Presidential campaign.

Election Integrity: In the run-up to the 2016 elections, we were focused on the kinds of cybersecurity attacks typically used by nation states, for example phishing and malware attacks. And we were too slow to spot information operations interference. Since then, we've made important changes to prevent bad actors from using misinformation to undermine the democratic process. This will never be a solved problem because we're up against determined, creative and well-funded adversaries. But we are making steady progress. Here is a list of the 10 most important changes we have made:

- **Ads transparency.** Advertising should be transparent: users should be able to see all the ads an advertiser is currently running on Facebook, Instagram and Messenger. And for ads with political content, we've created an archive that will hold ads with political content for seven years—including information about ad impressions and spend, as well as demographic data such as age, gender and location. People in Canada and Ireland have

already been able to see all the ads that a Page is running on Facebook—and we've launched this globally.

- **Verification and labeling.** Every advertiser will now need to confirm their ID and location before being able to run any ads with political content in the US. All ads with political content will also clearly state who paid for them.

- **Updating targeting.** We want ads on Facebook to be safe and civil. We thoroughly review the targeting criteria advertisers can use to ensure they are consistent with our principles. As a result, we removed nearly one-third of the targeting segments used by the IRA. We continue to allow some criteria that people may find controversial. But we do see businesses marketing things like historical books, documentaries or television shows using them in legitimate ways.

- **Better technology.** Over the past year, we've gotten increasingly better at finding and disabling fake accounts. We now block millions of fake accounts each day as people try to create them—and before they've done any harm. This is thanks to improvements in machine learning and artificial intelligence, which can proactively identify suspicious behavior at a scale that was not possible before—without needing to look at the content itself.

- **Action to tackle fake news.** We are working hard to stop the spread of false news. We work with third-party fact-checking organizations to limit the spread of articles rated false. To reduce the spread of false news, we remove fake accounts and disrupt economic incentives for traffickers of misinformation. We also use various signals, including feedback from our community, to identify potential false news. In countries where we have partnerships with independent third-party fact-checkers, stories rated as false by those fact-checkers are shown lower in News Feed. If Pages or domains repeatedly create or share misinformation, we significantly reduce their distribution and remove their advertising rights. We also want to empower people to decide for themselves what to read, trust, and share. We promote news literacy and work to inform people with more context. For example, if third-party fact-checkers write articles about a news story, we show them immediately below the story in the Related Articles unit. We also notify people and Page Admins if they try to share a story, or have shared one in the past, that's been determined to be false. In addition to our own efforts, we're learning from academics, scaling our partnerships with third-party fact-checkers and talking to other organizations about how we can work together.

  A key focus is working to disrupt the economics of fake news. For example, preventing the creation of fake accounts that spread it, banning sites that engage in this behavior from using our ad products, and demoting articles found to be false by fact checkers in News Feed—causing it to lose 80% of its traffic. We now work with independent fact checkers in the US, France, Germany, Ireland, the Netherlands, Italy, Mexico, Colombia, India, Indonesia and the Philippines with plans to scale to more countries in the coming months.

- **Significant investments in security.** We're doubling the number of people working on safety and security from 10,000 last year to over 20,000 this year. We expect these investments to impact our profitability. But the safety of people using Facebook needs to come before profit.

- **Industry collaboration.** Recently, we joined 34 global tech and security companies in signing a TechAccord pact to help improve security for everyone.

- **Information sharing and reporting channels.** In the 2017 German elections, we worked closely with the authorities there, including the Federal Office for Information Security (BSI). This gave them a dedicated reporting channel for security issues related to the federal elections.

- **Tracking 40+ elections.** In recent months, we've started to deploy new tools and teams to proactively identify threats in the run-up to specific elections. We first tested this effort during the Alabama Senate election, and plan to continue these efforts for elections around the globe, including the US midterms. Last year we used public service announcements to help inform people about fake news in 21 separate countries, including in advance of French, Kenyan and German elections.

- **Action against the Russia-based IRA.** In April, we removed 70 Facebook and 65 Instagram accounts—as well as 138 Facebook Pages—controlled by the IRA primarily targeted either at people living in Russia or Russian-speakers around the world including from neighboring countries like Azerbaijan, Uzbekistan and Ukraine. The IRA has repeatedly used complex networks of inauthentic accounts to deceive and manipulate people in the US, Europe and Russia—and we don't want them on Facebook anywhere in the world.

308. How, short of regulation, can Facebook prevent bad actors from undermining trust in democracy?

We want our platform to be a place where people can have authentic conversations about elections and other political topics. We believe this kind of engagement promotes democracy, but we know that there are actors working to interfere with those conversations and undermine our elections. We are already taking steps to proactively prevent election interference and we are strengthening these protections going forward.

Engagement with campaigns: We want all candidates, groups, and voters to use our platform to engage in elections. We want it to be easy for people to find, follow, and contact their elected representatives—and those running to represent them. That's why, for candidates across the political spectrum, Facebook offers the same levels of support in key moments to help campaigns understand how best to use the platform. Both the Obama and Romney campaigns had access to the same tools, and no campaign received any special treatment from Facebook. Likewise, we offered identical support to both the Trump and Clinton campaigns, and had teams assigned to both. Everyone had access to the same tools, which are the same tools that every campaign is offered, and is consistent with support provided to commercial clients in the normal course of business. Facebook representatives advise political advertisers on Facebook, as they

would with other, non-political managed accounts. We have a compliance team that trains our sales representatives to comply with all federal election law requirements in this area.

While no one from Facebook was assigned full-time to the Trump campaign, Facebook employees did interact with Cambridge Analytica employees. While our investigation is ongoing, our review indicates that Facebook employees did not identify any issues involving the improper use of Facebook data in the course of their interactions with Cambridge Analytica during the 2016 US Presidential campaign.

Election Integrity: In the run-up to the 2016 elections, we were focused on the kinds of cybersecurity attacks typically used by nation states, for example phishing and malware attacks. And we were too slow to spot information operations interference. Since then, we've made important changes to prevent bad actors from using misinformation to undermine the democratic process. This will never be a solved problem because we're up against determined, creative and well-funded adversaries. But we are making steady progress. Here is a list of the 10 most important changes we have made:

- **Ads transparency.** Advertising should be transparent: users should be able to see all the ads an advertiser is currently running on Facebook, Instagram and Messenger. And for ads with political content, we've created an archive that will hold ads with political content for seven years—including information about ad impressions and spend, as well as demographic data such as age, gender and location. People in Canada and Ireland have already been able to see all the ads that a Page is running on Facebook—and we've launched this globally.

- **Verification and labeling.** Every advertiser will now need to confirm their ID and location before being able to run any ads with political content in the US. All ads with political content will also clearly state who paid for them.

- **Updating targeting.** We want ads on Facebook to be safe and civil. We thoroughly review the targeting criteria advertisers can use to ensure they are consistent with our principles. As a result, we removed nearly one-third of the targeting segments used by the IRA. We continue to allow some criteria that people may find controversial. But we do see businesses marketing things like historical books, documentaries or television shows using them in legitimate ways.

- **Better technology.** Over the past year, we've gotten increasingly better at finding and disabling fake accounts. We now block millions of fake accounts each day as people try to create them—and before they've done any harm. This is thanks to improvements in machine learning and artificial intelligence, which can proactively identify suspicious behavior at a scale that was not possible before—without needing to look at the content itself.

- **Action to tackle fake news.** We are working hard to stop the spread of false news. We work with third-party fact-checking organizations to limit the spread of articles rated false. To reduce the spread of false news, we remove fake accounts and disrupt economic incentives for traffickers of misinformation. We also use various signals, including

feedback from our community, to identify potential false news. In countries where we have partnerships with independent third-party fact-checkers, stories rated as false by those fact-checkers are shown lower in News Feed. If Pages or domains repeatedly create or share misinformation, we significantly reduce their distribution and remove their advertising rights. We also want to empower people to decide for themselves what to read, trust, and share. We promote news literacy and work to inform people with more context. For example, if third-party fact-checkers write articles about a news story, we show them immediately below the story in the Related Articles unit. We also notify people and Page Admins if they try to share a story, or have shared one in the past, that's been determined to be false. In addition to our own efforts, we're learning from academics, scaling our partnerships with third-party fact-checkers and talking to other organizations about how we can work together.

A key focus is working to disrupt the economics of fake news. For example, preventing the creation of fake accounts that spread it, banning sites that engage in this behavior from using our ad products, and demoting articles found to be false by fact checkers in News Feed—causing it to lose 80% of its traffic. We now work with independent fact checkers in the US, France, Germany, Ireland, the Netherlands, Italy, Mexico, Colombia, India, Indonesia and the Philippines with plans to scale to more countries in the coming months.

- **Significant investments in security.** We're doubling the number of people working on safety and security from 10,000 last year to over 20,000 this year. We expect these investments to impact our profitability. But the safety of people using Facebook needs to come before profit.

- **Industry collaboration.** Recently, we joined 34 global tech and security companies in signing a TechAccord pact to help improve security for everyone.

- **Information sharing and reporting channels.** In the 2017 German elections, we worked closely with the authorities there, including the Federal Office for Information Security (BSI). This gave them a dedicated reporting channel for security issues related to the federal elections.

- **Tracking 40+ elections.** In recent months, we've started to deploy new tools and teams to proactively identify threats in the run-up to specific elections. We first tested this effort during the Alabama Senate election, and plan to continue these efforts for elections around the globe, including the US midterms. Last year we used public service announcements to help inform people about fake news in 21 separate countries, including in advance of French, Kenyan and German elections.

- **Action against the Russia-based IRA.** In April, we removed 70 Facebook and 65 Instagram accounts—as well as 138 Facebook Pages—controlled by the IRA primarily targeted either at people living in Russia or Russian-speakers around the world including from neighboring countries like Azerbaijan, Uzbekistan and Ukraine. The IRA has repeatedly used complex networks of inauthentic accounts to deceive and manipulate

people in the US, Europe and Russia—and we don't want them on Facebook anywhere in the world.

309. Where is the due diligence in marketing/sales when accepting foreign accounts, i.e. Russia???

For years, we had been aware of other types of activity that appeared to come from Russian sources—largely traditional security threats such as attacking people's accounts or using social media platforms to spread stolen information. What we saw early in the 2016 campaign cycle followed this pattern. Our security team that focuses on threat intelligence—which investigates advanced security threats as part of our overall information security organization—was, from the outset, alert to the possibility of Russian activity. In several instances before November 8, 2016, this team detected and mitigated threats from actors with ties to Russia and reported them to US law enforcement officials. This included activity from a cluster of accounts we had assessed to belong to a group (APT28) that the US government has publicly linked to Russian military intelligence services. This activity, which was aimed at employees of major US political parties, fell into the normal categories of offensive cyber activities we monitor for. We warned the targets who were at highest risk, and were later in contact with law enforcement authorities about this activity.

Later in the summer we also started to see a new kind of behavior from APT28-related accounts—namely, the creation of fake personas that were then used to seed stolen information to journalists. These fake personas were organized under the banner of an organization that called itself DC Leaks. This activity violated our policies, and we removed the DC Leaks accounts.

Facebook learned from press accounts and statements by congressional leaders that Russian actors might have tried to interfere in the 2016 election by exploiting Facebook's ad tools. This is not something we had seen before, and so we started an investigation. We found that fake accounts associated with the IRA tried to influence the election.

This will never be a solved problem because we're up against determined, creative and well-funded adversaries. But we are making steady progress in preventing bad actors from using misinformation to undermine the democratic process, such as: increased ad transparency, advertiser verification and labeling, updating targeting criteria, better technological efforts to find and disable fake accounts, third-party fact checking to stop the spread of false news, doubling the number of people working on safety and security, greater industry collaboration, increased information sharing and reporting channels, proactive identification of election threats, and specific action against the Russia-based IRA.

We will continue to work with the government, and across the tech industry and civil society, to address this important national security matter so that we can do our part to prevent similar abuse from happening again.

310. How is your company going to actively combat Russian interference in our democratic process?

For years, we had been aware of other types of activity that appeared to come from Russian sources—largely traditional security threats such as attacking people's accounts or using social media platforms to spread stolen information. What we saw early in the 2016 campaign cycle followed this pattern. Our security team that focuses on threat intelligence—which investigates advanced security threats as part of our overall information security organization—was, from the outset, alert to the possibility of Russian activity. In several instances before November 8, 2016, this team detected and mitigated threats from actors with ties to Russia and reported them to US law enforcement officials. This included activity from a cluster of accounts we had assessed to belong to a group (APT28) that the US government has publicly linked to Russian military intelligence services. This activity, which was aimed at employees of major US political parties, fell into the normal categories of offensive cyber activities we monitor for. We warned the targets who were at highest risk, and were later in contact with law enforcement authorities about this activity.

Later in the summer we also started to see a new kind of behavior from APT28-related accounts—namely, the creation of fake personas that were then used to seed stolen information to journalists. These fake personas were organized under the banner of an organization that called itself DC Leaks. This activity violated our policies, and we removed the DC Leaks accounts.

Facebook learned from press accounts and statements by congressional leaders that Russian actors might have tried to interfere in the 2016 election by exploiting Facebook's ad tools. This is not something we had seen before, and so we started an investigation. We found that fake accounts associated with the IRA tried to influence the election.

This will never be a solved problem because we're up against determined, creative and well-funded adversaries. But we are making steady progress in preventing bad actors from using misinformation to undermine the democratic process, such as: increased ad transparency, advertiser verification and labeling, updating targeting criteria, better technological efforts to find and disable fake accounts, third-party fact checking to stop the spread of false news, doubling the number of people working on safety and security, greater industry collaboration, increased information sharing and reporting channels, proactive identification of election threats, and specific action against the Russia-based IRA.

We will continue to work with the government, and across the tech industry and civil society, to address this important national security matter so that we can do our part to prevent similar abuse from happening again.

311. What type of FB person were the 3rd parties looking for? For what reason? What did they do with the information?

Facebook's policies regarding third-party usage of its platform technologies have prohibited—and continue to prohibit—third-party app developers from selling or licensing user data accessed from Facebook and from sharing any user data accessed from Facebook with any ad network, data broker or other advertising or monetization-related service. We take action on potential violations of our Platform Policies based on proactive review, external reports, and

other signals. Kogan was not permitted to sell or transfer data to third-parties for the purposes he did. In doing so, Kogan and his company violated Facebook's Platform Policies.

On December 11, 2015, *The Guardian* published an article reporting that Kogan and his company, GSR, may have passed information the app had obtained from Facebook users to SCL Elections Ltd. (SCL)/Cambridge Analytica. Facebook immediately banned Kogan's app from our platform and investigated what happened and what further action Facebook should take to enforce our Platform Policies. Facebook considered the matter closed after obtaining written certifications and confirmations from Kogan, GSR, Cambridge Analytica, and SCL declaring that all such data they had obtained was accounted for and destroyed. We did not have any reason to affirmatively question the veracity of any of these certifications until March 2018, when we learned from media reporting that questions had been raised concerning the accuracy of the certifications. Facebook immediately banned Cambridge Analytica and SCL from purchasing advertisements on our services as well as removed the personal accounts of some of their officers. Moreover, while Facebook's policies in place at the time allowed us to audit apps to ensure that they were safe and did not violate its terms, we had already terminated Kogan's app's access to Facebook. Accordingly, there were no ongoing concerns about the level of data that app could access or might access in the future. With the benefit of hindsight, we wish we had notified people whose information may have been impacted. Facebook has since notified all people potentially impacted with a detailed notice at the top of their News Feed.

312. What is Facebook currently doing to prevent malicious actors from gaining access to users' data?

Facebook's policies regarding third-party usage of its platform technologies have prohibited—and continue to prohibit—third-party app developers from selling or licensing user data obtained from Facebook and from sharing any user data obtained from Facebook with any ad network, data broker or other advertising or monetization-related service.

We use a variety of tools to enforce Facebook policies against violating parties, including developers. We review tens of thousands of apps per year and regularly disapprove noncompliant apps as part of our proactive review process. We also use tools like cease and desist letters, account suspensions, letter agreements, and civil litigation. For example, since 2006, Facebook has sent over 1,150 cease-and-desist letters to over 1,600 targets. In 2017, we took action against about 370,000 apps, ranging from imposing certain restrictions to removal of the app from the platform. Moreover, we have required parties who have procured our data without authorization to delete that data. We have invested significant resources in these efforts.

Recently, we announced a number of additional steps we're taking to address concerns raised by Kogan's app.

- **Review our platform.** We will investigate all apps that had access to large amounts of data before the platform changes we announced in 2014, and we will audit any app where we identify suspicious activity. If we identify misuses of data, we'll take immediate action, including banning the app from our platform and pursuing legal action if appropriate.

- **Tell people about data misuse.** We will tell people about apps that have misused their data. This includes building a way for people to know if their data might have been accessed via the app. Moving forward, if we remove an app, we will tell people.

- **Turn off access for unused apps.** If someone has not used an app within the last three months, we will turn off the app's access to their data.

- **Restrict Facebook Login data.** We are changing Login, so that the only data that an app can request without app review will include name, profile photo, and email address. Requesting any other data will require approval from Facebook. We will also no longer allow apps to ask for access to information like religious or political views, relationship status and details, custom friends lists, education and work history, fitness activity, book reading and music listening activity, news reading, video watch activity, and games activity. We will encourage people to manage the apps they use. We already show people what apps their accounts are connected to and allow them to control what data they've permitted those apps to use. But we're making it easier for people to see what apps they use and the information they have shared with those apps.

- **Reward people who find vulnerabilities.** We launched the Data Abuse Bounty program so that people can report to us any misuses of data by app developers.

- **Update our policies.** We have updated our terms and Data Policy to explain how we use data and how data is shared with app developers.

313. What steps have you taken since the 2016 election to protect against these breaches in the future?

We want our platform to be a place where people can have authentic conversations about elections and other political topics. We believe this kind of engagement promotes democracy, but we know that there are actors working to interfere with those conversations and undermine our elections. We are already taking steps to proactively prevent election interference and we are strengthening these protections going forward.

Engagement with campaigns: We want all candidates, groups, and voters to use our platform to engage in elections. We want it to be easy for people to find, follow, and contact their elected representatives—and those running to represent them. That's why, for candidates across the political spectrum, Facebook offers the same levels of support in key moments to help campaigns understand how best to use the platform. Both the Obama and Romney campaigns had access to the same tools, and no campaign received any special treatment from Facebook. Likewise, we offered identical support to both the Trump and Clinton campaigns, and had teams assigned to both. Everyone had access to the same tools, which are the same tools that every campaign is offered, and is consistent with support provided to commercial clients in the normal course of business. Facebook representatives advise political advertisers on Facebook, as they would with other, non-political managed accounts. We have a compliance team that trains our sales representatives to comply with all federal election law requirements in this area.

While no one from Facebook was assigned full-time to the Trump campaign, Facebook employees did interact with Cambridge Analytica employees. While our investigation is ongoing, our review indicates that Facebook employees did not identify any issues involving the improper use of Facebook data in the course of their interactions with Cambridge Analytica during the 2016 US Presidential campaign.

Election Integrity: In the run-up to the 2016 elections, we were focused on the kinds of cybersecurity attacks typically used by nation states, for example phishing and malware attacks. And we were too slow to spot information operations interference. Since then, we've made important changes to prevent bad actors from using misinformation to undermine the democratic process. This will never be a solved problem because we're up against determined, creative and well-funded adversaries. But we are making steady progress. Here is a list of the 10 most important changes we have made:

- **Ads transparency.** Advertising should be transparent: users should be able to see all the ads an advertiser is currently running on Facebook, Instagram and Messenger. And for ads with political content, we've created an archive that will hold ads with political content for seven years—including information about ad impressions and spend, as well as demographic data such as age, gender and location. People in Canada and Ireland have already been able to see all the ads that a Page is running on Facebook—and we've launched this globally.

- **Verification and labeling.** Every advertiser will now need to confirm their ID and location before being able to run any ads with political content in the US. All ads with political content will also clearly state who paid for them.

- **Updating targeting.** We want ads on Facebook to be safe and civil. We thoroughly review the targeting criteria advertisers can use to ensure they are consistent with our principles. As a result, we removed nearly one-third of the targeting segments used by the IRA. We continue to allow some criteria that people may find controversial. But we do see businesses marketing things like historical books, documentaries or television shows using them in legitimate ways.

- **Better technology.** Over the past year, we've gotten increasingly better at finding and disabling fake accounts. We now block millions of fake accounts each day as people try to create them—and before they've done any harm. This is thanks to improvements in machine learning and artificial intelligence, which can proactively identify suspicious behavior at a scale that was not possible before—without needing to look at the content itself.

- **Action to tackle fake news.** We are working hard to stop the spread of false news. We work with third-party fact-checking organizations to limit the spread of articles rated false. To reduce the spread of false news, we remove fake accounts and disrupt economic incentives for traffickers of misinformation. We also use various signals, including feedback from our community, to identify potential false news. In countries where we have partnerships with independent third-party fact-checkers, stories rated as false by those fact-checkers are shown lower in News Feed. If Pages or domains repeatedly create

or share misinformation, we significantly reduce their distribution and remove their advertising rights. We also want to empower people to decide for themselves what to read, trust, and share. We promote news literacy and work to inform people with more context. For example, if third-party fact-checkers write articles about a news story, we show them immediately below the story in the Related Articles unit. We also notify people and Page Admins if they try to share a story, or have shared one in the past, that's been determined to be false. In addition to our own efforts, we're learning from academics, scaling our partnerships with third-party fact-checkers and talking to other organizations about how we can work together.

A key focus is working to disrupt the economics of fake news. For example, preventing the creation of fake accounts that spread it, banning sites that engage in this behavior from using our ad products, and demoting articles found to be false by fact checkers in News Feed—causing it to lose 80% of its traffic. We now work with independent fact checkers in the US, France, Germany, Ireland, the Netherlands, Italy, Mexico, Colombia, India, Indonesia and the Philippines with plans to scale to more countries in the coming months.

- **Significant investments in security.** We're doubling the number of people working on safety and security from 10,000 last year to over 20,000 this year. We expect these investments to impact our profitability. But the safety of people using Facebook needs to come before profit.

- **Industry collaboration.** Recently, we joined 34 global tech and security companies in signing a TechAccord pact to help improve security for everyone.

- **Information sharing and reporting channels.** In the 2017 German elections, we worked closely with the authorities there, including the Federal Office for Information Security (BSI). This gave them a dedicated reporting channel for security issues related to the federal elections.

- **Tracking 40+ elections.** In recent months, we've started to deploy new tools and teams to proactively identify threats in the run-up to specific elections. We first tested this effort during the Alabama Senate election, and plan to continue these efforts for elections around the globe, including the US midterms. Last year we used public service announcements to help inform people about fake news in 21 separate countries, including in advance of French, Kenyan and German elections.

- **Action against the Russia-based IRA.** In April, we removed 70 Facebook and 65 Instagram accounts—as well as 138 Facebook Pages—controlled by the IRA primarily targeted either at people living in Russia or Russian-speakers around the world including from neighboring countries like Azerbaijan, Uzbekistan and Ukraine. The IRA has repeatedly used complex networks of inauthentic accounts to deceive and manipulate people in the US, Europe and Russia—and we don't want them on Facebook anywhere in the world.

314. In addition to what Facebook has already done since the 2016 Russian meddling in our election (which is a bipartisan issue), what else is Facebook doing to ensure this kind of attack does not happen again?

For years, we had been aware of other types of activity that appeared to come from Russian sources—largely traditional security threats such as attacking people's accounts or using social media platforms to spread stolen information. What we saw early in the 2016 campaign cycle followed this pattern. Our security team that focuses on threat intelligence—which investigates advanced security threats as part of our overall information security organization—was, from the outset, alert to the possibility of Russian activity. In several instances before November 8, 2016, this team detected and mitigated threats from actors with ties to Russia and reported them to US law enforcement officials. This included activity from a cluster of accounts we had assessed to belong to a group (APT28) that the US government has publicly linked to Russian military intelligence services. This activity, which was aimed at employees of major US political parties, fell into the normal categories of offensive cyber activities we monitor for. We warned the targets who were at highest risk, and were later in contact with law enforcement authorities about this activity.

Later in the summer we also started to see a new kind of behavior from APT28-related accounts—namely, the creation of fake personas that were then used to seed stolen information to journalists. These fake personas were organized under the banner of an organization that called itself DC Leaks. This activity violated our policies, and we removed the DC Leaks accounts.

Facebook learned from press accounts and statements by congressional leaders that Russian actors might have tried to interfere in the 2016 election by exploiting Facebook's ad tools. This is not something we had seen before, and so we started an investigation. We found that fake accounts associated with the IRA tried to influence the election.

This will never be a solved problem because we're up against determined, creative and well-funded adversaries. But we are making steady progress in preventing bad actors from using misinformation to undermine the democratic process, such as: increased ad transparency, advertiser verification and labeling, updating targeting criteria, better technological efforts to find and disable fake accounts, third-party fact checking to stop the spread of false news, doubling the number of people working on safety and security, greater industry collaboration, increased information sharing and reporting channels, proactive identification of election threats, and specific action against the Russia-based IRA.

We will continue to work with the government, and across the tech industry and civil society, to address this important national security matter so that we can do our part to prevent similar abuse from happening again.

315. What concrete steps are being taken to insure that there will not be foreign influence in our democratic process?

For years, we had been aware of other types of activity that appeared to come from Russian sources—largely traditional security threats such as attacking people's accounts or using

social media platforms to spread stolen information. What we saw early in the 2016 campaign cycle followed this pattern. Our security team that focuses on threat intelligence—which investigates advanced security threats as part of our overall information security organization—was, from the outset, alert to the possibility of Russian activity. In several instances before November 8, 2016, this team detected and mitigated threats from actors with ties to Russia and reported them to US law enforcement officials. This included activity from a cluster of accounts we had assessed to belong to a group (APT28) that the US government has publicly linked to Russian military intelligence services. This activity, which was aimed at employees of major US political parties, fell into the normal categories of offensive cyber activities we monitor for. We warned the targets who were at highest risk, and were later in contact with law enforcement authorities about this activity.

Later in the summer we also started to see a new kind of behavior from APT28-related accounts—namely, the creation of fake personas that were then used to seed stolen information to journalists. These fake personas were organized under the banner of an organization that called itself DC Leaks. This activity violated our policies, and we removed the DC Leaks accounts.

Facebook learned from press accounts and statements by congressional leaders that Russian actors might have tried to interfere in the 2016 election by exploiting Facebook's ad tools. This is not something we had seen before, and so we started an investigation. We found that fake accounts associated with the IRA tried to influence the election.

This will never be a solved problem because we're up against determined, creative and well-funded adversaries. But we are making steady progress in preventing bad actors from using misinformation to undermine the democratic process, such as: increased ad transparency, advertiser verification and labeling, updating targeting criteria, better technological efforts to find and disable fake accounts, third-party fact checking to stop the spread of false news, doubling the number of people working on safety and security, greater industry collaboration, increased information sharing and reporting channels, proactive identification of election threats, and specific action against the Russia-based IRA.

We will continue to work with the government, and across the tech industry and civil society, to address this important national security matter so that we can do our part to prevent similar abuse from happening again.

316. In your opinion did FB content targeting and compromised personal data result in DT's electoral win?

We want our platform to be a place where people can have authentic conversations about elections and other political topics. We believe this kind of engagement promotes democracy, but we know that there are actors working to interfere with those conversations and undermine our elections. We are already taking steps to proactively prevent election interference and we are strengthening these protections going forward.

Engagement with campaigns: We want all candidates, groups, and voters to use our platform to engage in elections. We want it to be easy for people to find, follow, and contact

their elected representatives—and those running to represent them. That's why, for candidates across the political spectrum, Facebook offers the same levels of support in key moments to help campaigns understand how best to use the platform. Both the Obama and Romney campaigns had access to the same tools, and no campaign received any special treatment from Facebook. Likewise, we offered identical support to both the Trump and Clinton campaigns, and had teams assigned to both. Everyone had access to the same tools, which are the same tools that every campaign is offered, and is consistent with support provided to commercial clients in the normal course of business. Facebook representatives advise political advertisers on Facebook, as they would with other, non-political managed accounts. We have a compliance team that trains our sales representatives to comply with all federal election law requirements in this area.

While no one from Facebook was assigned full-time to the Trump campaign, Facebook employees did interact with Cambridge Analytica employees. While our investigation is ongoing, our review indicates that Facebook employees did not identify any issues involving the improper use of Facebook data in the course of their interactions with Cambridge Analytica during the 2016 US Presidential campaign.

Election Integrity: In the run-up to the 2016 elections, we were focused on the kinds of cybersecurity attacks typically used by nation states, for example phishing and malware attacks. And we were too slow to spot information operations interference. Since then, we've made important changes to prevent bad actors from using misinformation to undermine the democratic process. This will never be a solved problem because we're up against determined, creative and well-funded adversaries. But we are making steady progress. Here is a list of the 10 most important changes we have made:

- **Ads transparency.** Advertising should be transparent: users should be able to see all the ads an advertiser is currently running on Facebook, Instagram and Messenger. And for ads with political content, we've created an archive that will hold ads with political content for seven years—including information about ad impressions and spend, as well as demographic data such as age, gender and location. People in Canada and Ireland have already been able to see all the ads that a Page is running on Facebook—and we've launched this globally.

- **Verification and labeling.** Every advertiser will now need to confirm their ID and location before being able to run any ads with political content in the US. All ads with political content will also clearly state who paid for them.

- **Updating targeting.** We want ads on Facebook to be safe and civil. We thoroughly review the targeting criteria advertisers can use to ensure they are consistent with our principles. As a result, we removed nearly one-third of the targeting segments used by the IRA. We continue to allow some criteria that people may find controversial. But we do see businesses marketing things like historical books, documentaries or television shows using them in legitimate ways.

- **Better technology.** Over the past year, we've gotten increasingly better at finding and disabling fake accounts. We now block millions of fake accounts each day as people try to create them—and before they've done any harm. This is thanks to improvements in

machine learning and artificial intelligence, which can proactively identify suspicious behavior at a scale that was not possible before—without needing to look at the content itself.

- **Action to tackle fake news.** We are working hard to stop the spread of false news. We work with third-party fact-checking organizations to limit the spread of articles rated false. To reduce the spread of false news, we remove fake accounts and disrupt economic incentives for traffickers of misinformation. We also use various signals, including feedback from our community, to identify potential false news. In countries where we have partnerships with independent third-party fact-checkers, stories rated as false by those fact-checkers are shown lower in News Feed. If Pages or domains repeatedly create or share misinformation, we significantly reduce their distribution and remove their advertising rights. We also want to empower people to decide for themselves what to read, trust, and share. We promote news literacy and work to inform people with more context. For example, if third-party fact-checkers write articles about a news story, we show them immediately below the story in the Related Articles unit. We also notify people and Page Admins if they try to share a story, or have shared one in the past, that's been determined to be false. In addition to our own efforts, we're learning from academics, scaling our partnerships with third-party fact-checkers and talking to other organizations about how we can work together.

  A key focus is working to disrupt the economics of fake news. For example, preventing the creation of fake accounts that spread it, banning sites that engage in this behavior from using our ad products, and demoting articles found to be false by fact checkers in News Feed—causing it to lose 80% of its traffic. We now work with independent fact checkers in the US, France, Germany, Ireland, the Netherlands, Italy, Mexico, Colombia, India, Indonesia and the Philippines with plans to scale to more countries in the coming months.

- **Significant investments in security.** We're doubling the number of people working on safety and security from 10,000 last year to over 20,000 this year. We expect these investments to impact our profitability. But the safety of people using Facebook needs to come before profit.

- **Industry collaboration.** Recently, we joined 34 global tech and security companies in signing a TechAccord pact to help improve security for everyone.

- **Information sharing and reporting channels.** In the 2017 German elections, we worked closely with the authorities there, including the Federal Office for Information Security (BSI). This gave them a dedicated reporting channel for security issues related to the federal elections.

- **Tracking 40+ elections.** In recent months, we've started to deploy new tools and teams to proactively identify threats in the run-up to specific elections. We first tested this effort during the Alabama Senate election, and plan to continue these efforts for elections around the globe, including the US midterms. Last year we used public service

announcements to help inform people about fake news in 21 separate countries, including in advance of French, Kenyan and German elections.

- **Action against the Russia-based IRA.** In April, we removed 70 Facebook and 65 Instagram accounts—as well as 138 Facebook Pages—controlled by the IRA primarily targeted either at people living in Russia or Russian-speakers around the world including from neighboring countries like Azerbaijan, Uzbekistan and Ukraine. The IRA has repeatedly used complex networks of inauthentic accounts to deceive and manipulate people in the US, Europe and Russia—and we don't want them on Facebook anywhere in the world.

317. How will the company specifically monitor fake news and bots and protect user security?

We want Facebook to be a place where people can discover more news, information, and perspectives, and we are working to build products that help to that. Through our News Feed algorithm, we also work hard to actively reduce the distribution of clickbait, sensationalism, and misinformation, on the one hand, and to boost news and information from sources that are trusted, informative, and local, on the other hand.

We are focusing on four different strategies to address misinformation:

- **Strengthening enforcement of our authenticity policies.** We are investing heavily in new technology and hiring thousands more people to tackle the problem of inauthenticity on the platform. Fake accounts are often associated with false news, so this is an area that will have a huge impact on curbing the spread of inaccurate information.

- **Finding industry solutions.** All of us—from tech companies and media companies to newsrooms and classrooms—must work together to find industry solutions to strengthen the online news ecosystem and our own digital literacy. That's why we're collaborating with others who operate in this space. Last January, we announced The Facebook Journalism Project, an initiative that seeks to establish stronger ties between Facebook and the news industry. The project is focused on developing news products, providing training and tools for journalists, and working with publishers and educators on how we can equip people with the knowledge they need to be informed readers in the digital age. Since launching the Journalism Project, we've met with more than 2,600 publishers around the world to understand how they use our products and how we can make improvements to better support their needs.

- **Disrupting economic incentives.** When it comes to fighting false news, we've found that a lot of it is financially motivated. So, one of the most effective approaches is removing the economic incentives for those who traffic in inaccurate information. We've done things like block ads from pages that repeatedly share false news and significantly limit the distribution of web pages that deliver low quality web experiences.

- **Building new products.** We believe it's important to amplify the good effects of social media and mitigate the bad—to contribute to the diversity of ideas, information, and view points, while strengthening our common understanding.

- We believe giving people more context can help them decide what to trust and what to share. The third-party fact-checking program we have developed uses reports from our community, along with other signals, to send stories to accredited third-party fact checking organizations. If the fact checking organizations identify a story as fake, we will suggest related articles in News Feed to show people different points of view, including information from fact checkers. Stories that have been disputed may also appear lower in News Feed. Our own data analytics show that a false rating from one of our fact checking partners reduces future impressions on Facebook by 80 percent.

- We're also testing Article Context as a way of giving people more information about the material they're reading on Facebook. Since we launched this test, some of the articles people see in News Feed will feature an "i" icon that allows them to access more information at the tap of a button. The information we surface is pulled from across the internet, and includes things like the publisher's Wikipedia entry, trending articles or related articles about the topic, and information about how the article is being shared on Facebook. In some cases, if that information is unavailable, we will let people know since that can also be helpful context.

318. Does Facebook have a duty to prevent the use of its platform from undermining elections? Is transparency the right antidote?

We want our platform to be a place where people can have authentic conversations about elections and other political topics. We believe this kind of engagement promotes democracy, but we know that there are actors working to interfere with those conversations and undermine our elections. We are already taking steps to proactively prevent election interference and we are strengthening these protections going forward.

Engagement with campaigns: We want all candidates, groups, and voters to use our platform to engage in elections. We want it to be easy for people to find, follow, and contact their elected representatives—and those running to represent them. That's why, for candidates across the political spectrum, Facebook offers the same levels of support in key moments to help campaigns understand how best to use the platform. Both the Obama and Romney campaigns had access to the same tools, and no campaign received any special treatment from Facebook. Likewise, we offered identical support to both the Trump and Clinton campaigns, and had teams assigned to both. Everyone had access to the same tools, which are the same tools that every campaign is offered, and is consistent with support provided to commercial clients in the normal course of business. Facebook representatives advise political advertisers on Facebook, as they would with other, non-political managed accounts. We have a compliance team that trains our sales representatives to comply with all federal election law requirements in this area.

While no one from Facebook was assigned full-time to the Trump campaign, Facebook employees did interact with Cambridge Analytica employees. While our investigation is ongoing, our review indicates that Facebook employees did not identify any issues involving the improper use of Facebook data in the course of their interactions with Cambridge Analytica during the 2016 US Presidential campaign.

Election Integrity: In the run-up to the 2016 elections, we were focused on the kinds of cybersecurity attacks typically used by nation states, for example phishing and malware attacks. And we were too slow to spot information operations interference. Since then, we've made important changes to prevent bad actors from using misinformation to undermine the democratic process. This will never be a solved problem because we're up against determined, creative and well-funded adversaries. But we are making steady progress. Here is a list of the 10 most important changes we have made:

- **Ads transparency.** Advertising should be transparent: users should be able to see all the ads an advertiser is currently running on Facebook, Instagram and Messenger. And for ads with political content, we've created an archive that will hold ads with political content for seven years—including information about ad impressions and spend, as well as demographic data such as age, gender and location. People in Canada and Ireland have already been able to see all the ads that a Page is running on Facebook—and we've launched this globally.

- **Verification and labeling.** Every advertiser will now need to confirm their ID and location before being able to run any ads with political content in the US. All ads with political content will also clearly state who paid for them.

- **Updating targeting.** We want ads on Facebook to be safe and civil. We thoroughly review the targeting criteria advertisers can use to ensure they are consistent with our principles. As a result, we removed nearly one-third of the targeting segments used by the IRA. We continue to allow some criteria that people may find controversial. But we do see businesses marketing things like historical books, documentaries or television shows using them in legitimate ways.

- **Better technology.** Over the past year, we've gotten increasingly better at finding and disabling fake accounts. We now block millions of fake accounts each day as people try to create them—and before they've done any harm. This is thanks to improvements in machine learning and artificial intelligence, which can proactively identify suspicious behavior at a scale that was not possible before—without needing to look at the content itself.

- **Action to tackle fake news.** We are working hard to stop the spread of false news. We work with third-party fact-checking organizations to limit the spread of articles rated false. To reduce the spread of false news, we remove fake accounts and disrupt economic incentives for traffickers of misinformation. We also use various signals, including feedback from our community, to identify potential false news. In countries where we have partnerships with independent third-party fact-checkers, stories rated as false by those fact-checkers are shown lower in News Feed. If Pages or domains repeatedly create or share misinformation, we significantly reduce their distribution and remove their advertising rights. We also want to empower people to decide for themselves what to read, trust, and share. We promote news literacy and work to inform people with more context. For example, if third-party fact-checkers write articles about a news story, we show them immediately below the story in the Related Articles unit. We also notify people and Page Admins if they try to share a story, or have shared one in the past, that's

been determined to be false. In addition to our own efforts, we're learning from academics, scaling our partnerships with third-party fact-checkers and talking to other organizations about how we can work together.

A key focus is working to disrupt the economics of fake news. For example, preventing the creation of fake accounts that spread it, banning sites that engage in this behavior from using our ad products, and demoting articles found to be false by fact checkers in News Feed—causing it to lose 80% of its traffic. We now work with independent fact checkers in the US, France, Germany, Ireland, the Netherlands, Italy, Mexico, Colombia, India, Indonesia and the Philippines with plans to scale to more countries in the coming months.

- **Significant investments in security.** We're doubling the number of people working on safety and security from 10,000 last year to over 20,000 this year. We expect these investments to impact our profitability. But the safety of people using Facebook needs to come before profit.

- **Industry collaboration.** Recently, we joined 34 global tech and security companies in signing a TechAccord pact to help improve security for everyone.

- **Information sharing and reporting channels.** In the 2017 German elections, we worked closely with the authorities there, including the Federal Office for Information Security (BSI). This gave them a dedicated reporting channel for security issues related to the federal elections.

- **Tracking 40+ elections.** In recent months, we've started to deploy new tools and teams to proactively identify threats in the run-up to specific elections. We first tested this effort during the Alabama Senate election, and plan to continue these efforts for elections around the globe, including the US midterms. Last year we used public service announcements to help inform people about fake news in 21 separate countries, including in advance of French, Kenyan and German elections.

- **Action against the Russia-based IRA.** In April, we removed 70 Facebook and 65 Instagram accounts—as well as 138 Facebook Pages—controlled by the IRA primarily targeted either at people living in Russia or Russian-speakers around the world including from neighboring countries like Azerbaijan, Uzbekistan and Ukraine. The IRA has repeatedly used complex networks of inauthentic accounts to deceive and manipulate people in the US, Europe and Russia—and we don't want them on Facebook anywhere in the world.

319. Why did Facebook sell all of our private information? Was it to further Trump's campaign?

We believe everyone deserves good privacy controls. A user owns the information they share on Facebook. This means they decide what they share and who they share it with on Facebook, and they can change their mind. We require websites and apps who use our tools to

tell users they're collecting and sharing their information with us, and to get users' permission to do so.

Everyone has the right to expect strong protections for their information. We also need to do our part to help keep our community safe, in a way that's consistent with people's privacy expectations. We've recently announced several steps to give people more control over their privacy, including a new Privacy Shortcuts tool that we're rolling out now to give people information about how to control their information, including choosing who can see what they post and adding protections like two-factor authentication to their account. People can learn more about how to protect their privacy in our updated Data Policy and in our Privacy Basics feature (https://www.facebook.com/about/basics).

We are in the process of investigating every app that had access to a large amount of information before we changed our Platform in 2014. The investigation process is in full swing. We have large teams of internal and external experts working hard to investigate these apps as quickly as possible. As of early June 2018, thousands of apps have been investigated and around 200 apps have been suspended—pending a thorough investigation into whether they did in fact misuse any data. Where we find evidence that these or other apps did misuse data, we will ban them and let people know.

Facebook is generally not opposed to regulation but wants to ensure it is the right regulation. The issues facing the industry are complex, multi-faceted, and affect an important part of peoples' lives. As such, Facebook is absolutely committed to working with regulators, like Congress, to craft the right regulations. Facebook would be happy to review any proposed legislation and provide comments.

320. How will you prevent Russians and anybody from weaponizing Facebook for improper uses?

For years, we had been aware of other types of activity that appeared to come from Russian sources—largely traditional security threats such as attacking people's accounts or using social media platforms to spread stolen information. What we saw early in the 2016 campaign cycle followed this pattern. Our security team that focuses on threat intelligence—which investigates advanced security threats as part of our overall information security organization—was, from the outset, alert to the possibility of Russian activity. In several instances before November 8, 2016, this team detected and mitigated threats from actors with ties to Russia and reported them to US law enforcement officials. This included activity from a cluster of accounts we had assessed to belong to a group (APT28) that the US government has publicly linked to Russian military intelligence services. This activity, which was aimed at employees of major US political parties, fell into the normal categories of offensive cyber activities we monitor for. We warned the targets who were at highest risk, and were later in contact with law enforcement authorities about this activity.

Later in the summer we also started to see a new kind of behavior from APT28-related accounts—namely, the creation of fake personas that were then used to seed stolen information to journalists. These fake personas were organized under the banner of an organization that

called itself DC Leaks. This activity violated our policies, and we removed the DC Leaks accounts.

Facebook learned from press accounts and statements by congressional leaders that Russian actors might have tried to interfere in the 2016 election by exploiting Facebook's ad tools. This is not something we had seen before, and so we started an investigation. We found that fake accounts associated with the IRA tried to influence the election.

This will never be a solved problem because we're up against determined, creative and well-funded adversaries. But we are making steady progress in preventing bad actors from using misinformation to undermine the democratic process, such as: increased ad transparency, advertiser verification and labeling, updating targeting criteria, better technological efforts to find and disable fake accounts, third-party fact checking to stop the spread of false news, doubling the number of people working on safety and security, greater industry collaboration, increased information sharing and reporting channels, proactive identification of election threats, and specific action against the Russia-based IRA.

We will continue to work with the government, and across the tech industry and civil society, to address this important national security matter so that we can do our part to prevent similar abuse from happening again.

321. So we heard, a couple of months ago, how your staff carefully explained to the Trump team how to use your system to get personal data on your subscribers and how to use it. Now you think we forgot how you handed them the store and that this was all some mistake or negligence? It wasn't a mistake. It was deliberate collusion.

We want our platform to be a place where people can have authentic conversations about elections and other political topics. We believe this kind of engagement promotes democracy, but we know that there are actors working to interfere with those conversations and undermine our elections. We are already taking steps to proactively prevent election interference and we are strengthening these protections going forward.

Engagement with campaigns: We want all candidates, groups, and voters to use our platform to engage in elections. We want it to be easy for people to find, follow, and contact their elected representatives—and those running to represent them. That's why, for candidates across the political spectrum, Facebook offers the same levels of support in key moments to help campaigns understand how best to use the platform. Both the Obama and Romney campaigns had access to the same tools, and no campaign received any special treatment from Facebook. Likewise, we offered identical support to both the Trump and Clinton campaigns, and had teams assigned to both. Everyone had access to the same tools, which are the same tools that every campaign is offered, and is consistent with support provided to commercial clients in the normal course of business. Facebook representatives advise political advertisers on Facebook, as they would with other, non-political managed accounts. We have a compliance team that trains our sales representatives to comply with all federal election law requirements in this area.

While no one from Facebook was assigned full-time to the Trump campaign, Facebook employees did interact with Cambridge Analytica employees. While our investigation is

ongoing, our review indicates that Facebook employees did not identify any issues involving the improper use of Facebook data in the course of their interactions with Cambridge Analytica during the 2016 US Presidential campaign.

Election Integrity: In the run-up to the 2016 elections, we were focused on the kinds of cybersecurity attacks typically used by nation states, for example phishing and malware attacks. And we were too slow to spot information operations interference. Since then, we've made important changes to prevent bad actors from using misinformation to undermine the democratic process. This will never be a solved problem because we're up against determined, creative and well-funded adversaries. But we are making steady progress. Here is a list of the 10 most important changes we have made:

- **Ads transparency.** Advertising should be transparent: users should be able to see all the ads an advertiser is currently running on Facebook, Instagram and Messenger. And for ads with political content, we've created an archive that will hold ads with political content for seven years—including information about ad impressions and spend, as well as demographic data such as age, gender and location. People in Canada and Ireland have already been able to see all the ads that a Page is running on Facebook—and we've launched this globally.

- **Verification and labeling.** Every advertiser will now need to confirm their ID and location before being able to run any ads with political content in the US. All ads with political content will also clearly state who paid for them.

- **Updating targeting.** We want ads on Facebook to be safe and civil. We thoroughly review the targeting criteria advertisers can use to ensure they are consistent with our principles. As a result, we removed nearly one-third of the targeting segments used by the IRA. We continue to allow some criteria that people may find controversial. But we do see businesses marketing things like historical books, documentaries or television shows using them in legitimate ways.

- **Better technology.** Over the past year, we've gotten increasingly better at finding and disabling fake accounts. We now block millions of fake accounts each day as people try to create them—and before they've done any harm. This is thanks to improvements in machine learning and artificial intelligence, which can proactively identify suspicious behavior at a scale that was not possible before—without needing to look at the content itself.

- **Action to tackle fake news.** We are working hard to stop the spread of false news. We work with third-party fact-checking organizations to limit the spread of articles rated false. To reduce the spread of false news, we remove fake accounts and disrupt economic incentives for traffickers of misinformation. We also use various signals, including feedback from our community, to identify potential false news. In countries where we have partnerships with independent third-party fact-checkers, stories rated as false by those fact-checkers are shown lower in News Feed. If Pages or domains repeatedly create or share misinformation, we significantly reduce their distribution and remove their advertising rights. We also want to empower people to decide for themselves what to

read, trust, and share. We promote news literacy and work to inform people with more context. For example, if third-party fact-checkers write articles about a news story, we show them immediately below the story in the Related Articles unit. We also notify people and Page Admins if they try to share a story, or have shared one in the past, that's been determined to be false. In addition to our own efforts, we're learning from academics, scaling our partnerships with third-party fact-checkers and talking to other organizations about how we can work together.

A key focus is working to disrupt the economics of fake news. For example, preventing the creation of fake accounts that spread it, banning sites that engage in this behavior from using our ad products, and demoting articles found to be false by fact checkers in News Feed—causing it to lose 80% of its traffic. We now work with independent fact checkers in the US, France, Germany, Ireland, the Netherlands, Italy, Mexico, Colombia, India, Indonesia and the Philippines with plans to scale to more countries in the coming months.

- **Significant investments in security.** We're doubling the number of people working on safety and security from 10,000 last year to over 20,000 this year. We expect these investments to impact our profitability. But the safety of people using Facebook needs to come before profit.

- **Industry collaboration.** Recently, we joined 34 global tech and security companies in signing a TechAccord pact to help improve security for everyone.

- **Information sharing and reporting channels.** In the 2017 German elections, we worked closely with the authorities there, including the Federal Office for Information Security (BSI). This gave them a dedicated reporting channel for security issues related to the federal elections.

- **Tracking 40+ elections.** In recent months, we've started to deploy new tools and teams to proactively identify threats in the run-up to specific elections. We first tested this effort during the Alabama Senate election, and plan to continue these efforts for elections around the globe, including the US midterms. Last year we used public service announcements to help inform people about fake news in 21 separate countries, including in advance of French, Kenyan and German elections.

- **Action against the Russia-based IRA.** In April, we removed 70 Facebook and 65 Instagram accounts—as well as 138 Facebook Pages—controlled by the IRA primarily targeted either at people living in Russia or Russian-speakers around the world including from neighboring countries like Azerbaijan, Uzbekistan and Ukraine. The IRA has repeatedly used complex networks of inauthentic accounts to deceive and manipulate people in the US, Europe and Russia—and we don't want them on Facebook anywhere in the world.

322. Did you allow the same access to President Obama's election team?

We want our platform to be a place where people can have authentic conversations about elections and other political topics. We believe this kind of engagement promotes democracy, but we know that there are actors working to interfere with those conversations and undermine our elections. We are already taking steps to proactively prevent election interference and we are strengthening these protections going forward.

Engagement with campaigns: We want all candidates, groups, and voters to use our platform to engage in elections. We want it to be easy for people to find, follow, and contact their elected representatives—and those running to represent them. That's why, for candidates across the political spectrum, Facebook offers the same levels of support in key moments to help campaigns understand how best to use the platform. Both the Obama and Romney campaigns had access to the same tools, and no campaign received any special treatment from Facebook. Likewise, we offered identical support to both the Trump and Clinton campaigns, and had teams assigned to both. Everyone had access to the same tools, which are the same tools that every campaign is offered, and is consistent with support provided to commercial clients in the normal course of business. Facebook representatives advise political advertisers on Facebook, as they would with other, non-political managed accounts. We have a compliance team that trains our sales representatives to comply with all federal election law requirements in this area.

While no one from Facebook was assigned full-time to the Trump campaign, Facebook employees did interact with Cambridge Analytica employees. While our investigation is ongoing, our review indicates that Facebook employees did not identify any issues involving the improper use of Facebook data in the course of their interactions with Cambridge Analytica during the 2016 US Presidential campaign.

Election Integrity: In the run-up to the 2016 elections, we were focused on the kinds of cybersecurity attacks typically used by nation states, for example phishing and malware attacks. And we were too slow to spot information operations interference. Since then, we've made important changes to prevent bad actors from using misinformation to undermine the democratic process. This will never be a solved problem because we're up against determined, creative and well-funded adversaries. But we are making steady progress. Here is a list of the 10 most important changes we have made:

- **Ads transparency.** Advertising should be transparent: users should be able to see all the ads an advertiser is currently running on Facebook, Instagram and Messenger. And for ads with political content, we've created an archive that will hold ads with political content for seven years—including information about ad impressions and spend, as well as demographic data such as age, gender and location. People in Canada and Ireland have already been able to see all the ads that a Page is running on Facebook—and we've launched this globally.

- **Verification and labeling.** Every advertiser will now need to confirm their ID and location before being able to run any ads with political content in the US. All ads with political content will also clearly state who paid for them.

- **Updating targeting.** We want ads on Facebook to be safe and civil. We thoroughly review the targeting criteria advertisers can use to ensure they are consistent with our

principles. As a result, we removed nearly one-third of the targeting segments used by the IRA. We continue to allow some criteria that people may find controversial. But we do see businesses marketing things like historical books, documentaries or television shows using them in legitimate ways.

- **Better technology.** Over the past year, we've gotten increasingly better at finding and disabling fake accounts. We now block millions of fake accounts each day as people try to create them—and before they've done any harm. This is thanks to improvements in machine learning and artificial intelligence, which can proactively identify suspicious behavior at a scale that was not possible before—without needing to look at the content itself.

- **Action to tackle fake news.** We are working hard to stop the spread of false news. We work with third-party fact-checking organizations to limit the spread of articles rated false. To reduce the spread of false news, we remove fake accounts and disrupt economic incentives for traffickers of misinformation. We also use various signals, including feedback from our community, to identify potential false news. In countries where we have partnerships with independent third-party fact-checkers, stories rated as false by those fact-checkers are shown lower in News Feed. If Pages or domains repeatedly create or share misinformation, we significantly reduce their distribution and remove their advertising rights. We also want to empower people to decide for themselves what to read, trust, and share. We promote news literacy and work to inform people with more context. For example, if third-party fact-checkers write articles about a news story, we show them immediately below the story in the Related Articles unit. We also notify people and Page Admins if they try to share a story, or have shared one in the past, that's been determined to be false. In addition to our own efforts, we're learning from academics, scaling our partnerships with third-party fact-checkers and talking to other organizations about how we can work together.

  A key focus is working to disrupt the economics of fake news. For example, preventing the creation of fake accounts that spread it, banning sites that engage in this behavior from using our ad products, and demoting articles found to be false by fact checkers in News Feed—causing it to lose 80% of its traffic. We now work with independent fact checkers in the US, France, Germany, Ireland, the Netherlands, Italy, Mexico, Colombia, India, Indonesia and the Philippines with plans to scale to more countries in the coming months.

- **Significant investments in security.** We're doubling the number of people working on safety and security from 10,000 last year to over 20,000 this year. We expect these investments to impact our profitability. But the safety of people using Facebook needs to come before profit.

- **Industry collaboration.** Recently, we joined 34 global tech and security companies in signing a TechAccord pact to help improve security for everyone.

- **Information sharing and reporting channels.** In the 2017 German elections, we worked closely with the authorities there, including the Federal Office for Information

Security (BSI). This gave them a dedicated reporting channel for security issues related to the federal elections.

- **Tracking 40+ elections.** In recent months, we've started to deploy new tools and teams to proactively identify threats in the run-up to specific elections. We first tested this effort during the Alabama Senate election, and plan to continue these efforts for elections around the globe, including the US midterms. Last year we used public service announcements to help inform people about fake news in 21 separate countries, including in advance of French, Kenyan and German elections.

- **Action against the Russia-based IRA.** In April, we removed 70 Facebook and 65 Instagram accounts—as well as 138 Facebook Pages—controlled by the IRA primarily targeted either at people living in Russia or Russian-speakers around the world including from neighboring countries like Azerbaijan, Uzbekistan and Ukraine. The IRA has repeatedly used complex networks of inauthentic accounts to deceive and manipulate people in the US, Europe and Russia—and we don't want them on Facebook anywhere in the world.

323. How has your position changed on the role Facebook is playing in our democracy?

We want our platform to be a place where people can have authentic conversations about elections and other political topics. We believe this kind of engagement promotes democracy, but we know that there are actors working to interfere with those conversations and undermine our elections. We are already taking steps to proactively prevent election interference and we are strengthening these protections going forward.

Engagement with campaigns: We want all candidates, groups, and voters to use our platform to engage in elections. We want it to be easy for people to find, follow, and contact their elected representatives—and those running to represent them. That's why, for candidates across the political spectrum, Facebook offers the same levels of support in key moments to help campaigns understand how best to use the platform. Both the Obama and Romney campaigns had access to the same tools, and no campaign received any special treatment from Facebook. Likewise, we offered identical support to both the Trump and Clinton campaigns, and had teams assigned to both. Everyone had access to the same tools, which are the same tools that every campaign is offered, and is consistent with support provided to commercial clients in the normal course of business. Facebook representatives advise political advertisers on Facebook, as they would with other, non-political managed accounts. We have a compliance team that trains our sales representatives to comply with all federal election law requirements in this area.

While no one from Facebook was assigned full-time to the Trump campaign, Facebook employees did interact with Cambridge Analytica employees. While our investigation is ongoing, our review indicates that Facebook employees did not identify any issues involving the improper use of Facebook data in the course of their interactions with Cambridge Analytica during the 2016 US Presidential campaign.

Election Integrity: In the run-up to the 2016 elections, we were focused on the kinds of cybersecurity attacks typically used by nation states, for example phishing and malware attacks.

And we were too slow to spot information operations interference. Since then, we've made important changes to prevent bad actors from using misinformation to undermine the democratic process. This will never be a solved problem because we're up against determined, creative and well-funded adversaries. But we are making steady progress. Here is a list of the 10 most important changes we have made:

- **Ads transparency.** Advertising should be transparent: users should be able to see all the ads an advertiser is currently running on Facebook, Instagram and Messenger. And for ads with political content, we've created an archive that will hold ads with political content for seven years—including information about ad impressions and spend, as well as demographic data such as age, gender and location. People in Canada and Ireland have already been able to see all the ads that a Page is running on Facebook—and we've launched this globally.

- **Verification and labeling.** Every advertiser will now need to confirm their ID and location before being able to run any ads with political content in the US. All ads with political content will also clearly state who paid for them.

- **Updating targeting.** We want ads on Facebook to be safe and civil. We thoroughly review the targeting criteria advertisers can use to ensure they are consistent with our principles. As a result, we removed nearly one-third of the targeting segments used by the IRA. We continue to allow some criteria that people may find controversial. But we do see businesses marketing things like historical books, documentaries or television shows using them in legitimate ways.

- **Better technology.** Over the past year, we've gotten increasingly better at finding and disabling fake accounts. We now block millions of fake accounts each day as people try to create them—and before they've done any harm. This is thanks to improvements in machine learning and artificial intelligence, which can proactively identify suspicious behavior at a scale that was not possible before—without needing to look at the content itself.

- **Action to tackle fake news.** We are working hard to stop the spread of false news. We work with third-party fact-checking organizations to limit the spread of articles rated false. To reduce the spread of false news, we remove fake accounts and disrupt economic incentives for traffickers of misinformation. We also use various signals, including feedback from our community, to identify potential false news. In countries where we have partnerships with independent third-party fact-checkers, stories rated as false by those fact-checkers are shown lower in News Feed. If Pages or domains repeatedly create or share misinformation, we significantly reduce their distribution and remove their advertising rights. We also want to empower people to decide for themselves what to read, trust, and share. We promote news literacy and work to inform people with more context. For example, if third-party fact-checkers write articles about a news story, we show them immediately below the story in the Related Articles unit. We also notify people and Page Admins if they try to share a story, or have shared one in the past, that's been determined to be false. In addition to our own efforts, we're learning from academics, scaling our partnerships with third-party fact-checkers and talking to other

organizations about how we can work together.

A key focus is working to disrupt the economics of fake news. For example, preventing the creation of fake accounts that spread it, banning sites that engage in this behavior from using our ad products, and demoting articles found to be false by fact checkers in News Feed—causing it to lose 80% of its traffic. We now work with independent fact checkers in the US, France, Germany, Ireland, the Netherlands, Italy, Mexico, Colombia, India, Indonesia and the Philippines with plans to scale to more countries in the coming months.

- **Significant investments in security.** We're doubling the number of people working on safety and security from 10,000 last year to over 20,000 this year. We expect these investments to impact our profitability. But the safety of people using Facebook needs to come before profit.

- **Industry collaboration.** Recently, we joined 34 global tech and security companies in signing a TechAccord pact to help improve security for everyone.

- **Information sharing and reporting channels.** In the 2017 German elections, we worked closely with the authorities there, including the Federal Office for Information Security (BSI). This gave them a dedicated reporting channel for security issues related to the federal elections.

- **Tracking 40+ elections.** In recent months, we've started to deploy new tools and teams to proactively identify threats in the run-up to specific elections. We first tested this effort during the Alabama Senate election, and plan to continue these efforts for elections around the globe, including the US midterms. Last year we used public service announcements to help inform people about fake news in 21 separate countries, including in advance of French, Kenyan and German elections.

- **Action against the Russia-based IRA.** In April, we removed 70 Facebook and 65 Instagram accounts—as well as 138 Facebook Pages—controlled by the IRA primarily targeted either at people living in Russia or Russian-speakers around the world including from neighboring countries like Azerbaijan, Uzbekistan and Ukraine. The IRA has repeatedly used complex networks of inauthentic accounts to deceive and manipulate people in the US, Europe and Russia—and we don't want them on Facebook anywhere in the world.

324. How can you recognize third parties that are malicious, if they are not well know?

Facebook's policies regarding third-party usage of its platform technologies have prohibited—and continue to prohibit—third-party app developers from selling or licensing user data obtained from Facebook and from sharing any user data obtained from Facebook with any ad network, data broker or other advertising or monetization-related service.

We use a variety of tools to enforce Facebook policies against violating parties, including developers. We review tens of thousands of apps per year and regularly disapprove noncompliant

apps as part of our proactive review process. We also use tools like cease and desist letters, account suspensions, letter agreements, and civil litigation. For example, since 2006, Facebook has sent over 1,150 cease-and-desist letters to over 1,600 targets. In 2017, we took action against about 370,000 apps, ranging from imposing certain restrictions to removal of the app from the platform. Moreover, we have required parties who have procured our data without authorization to delete that data. We have invested significant resources in these efforts.

Recently, we announced a number of additional steps we're taking to address concerns raised by Kogan's app.

- **Review our platform.** We will investigate all apps that had access to large amounts of data before the platform changes we announced in 2014, and we will audit any app where we identify suspicious activity. If we identify misuses of data, we'll take immediate action, including banning the app from our platform and pursuing legal action if appropriate.

- **Tell people about data misuse.** We will tell people about apps that have misused their data. This includes building a way for people to know if their data might have been accessed via the app. Moving forward, if we remove an app, we will tell people.

- **Turn off access for unused apps.** If someone has not used an app within the last three months, we will turn off the app's access to their data.

- **Restrict Facebook Login data.** We are changing Login, so that the only data that an app can request without app review will include name, profile photo, and email address. Requesting any other data will require approval from Facebook. We will also no longer allow apps to ask for access to information like religious or political views, relationship status and details, custom friends lists, education and work history, fitness activity, book reading and music listening activity, news reading, video watch activity, and games activity. We will encourage people to manage the apps they use. We already show people what apps their accounts are connected to and allow them to control what data they've permitted those apps to use. But we're making it easier for people to see what apps they use and the information they have shared with those apps.

- **Reward people who find vulnerabilities.** We launched the Data Abuse Bounty program so that people can report to us any misuses of data by app developers.

- **Update our policies.** We have updated our terms and Data Policy to explain how we use data and how data is shared with app developers.

325. How does he plan to balance advertising/data revenues v protecting privacy and combatting fake news

To build a secure product with extensive infrastructure that connects people wherever they live or whatever their income level, we need to make sure everyone can afford it. Advertising lets us keep Facebook free, which ensures it remains affordable for everyone. We also believe the ads you see across the Facebook family of apps and services should be useful

and relevant to you. Users can't opt out of seeing ads altogether because selling ads is what keeps Facebook free, but they do have different options to control how their data can and can't be used to show them ads. They're all found in ad preferences, which allows users to turn off the use of all data collected from partners off Facebook to target ads. Users can also decide which of their profile fields they want used for ad targeting in the Information section under "About you." Users can remove themselves from interests under "Your interests" and categories under "Your categories." And, we do not sell people's information to anyone, and we never will.

Facebook is committed to transparency for all ads, including ads with political content. Facebook believes that people should be able to easily understand why they are seeing ads, who paid for them, and what other ads those advertisers are running. As such, Facebook only allows authorized advertisers to run ads about elections or issues that are being debated across the country. In order to be authorized by Facebook, advertisers will need to confirm their identity and location. Furthermore, all political and issue ads will include a disclosure which reads: "Paid for by," and when users click on this disclosure they will be able to see details about the advertiser. Users will also be able to see an explanation of why they saw the particular ad. This is similar to the disclosure included on political TV advertisements. We just launched globally View Active Ads, a feature that will enable anyone to see all of the ads an advertiser is currently running by visiting the advertiser's Facebook Page.

326. Are they doing enough right now to protect Midterm elections?

We want our platform to be a place where people can have authentic conversations about elections and other political topics. We believe this kind of engagement promotes democracy, but we know that there are actors working to interfere with those conversations and undermine our elections. We are already taking steps to proactively prevent election interference and we are strengthening these protections going forward.

Engagement with campaigns: We want all candidates, groups, and voters to use our platform to engage in elections. We want it to be easy for people to find, follow, and contact their elected representatives—and those running to represent them. That's why, for candidates across the political spectrum, Facebook offers the same levels of support in key moments to help campaigns understand how best to use the platform. Both the Obama and Romney campaigns had access to the same tools, and no campaign received any special treatment from Facebook. Likewise, we offered identical support to both the Trump and Clinton campaigns, and had teams assigned to both. Everyone had access to the same tools, which are the same tools that every campaign is offered, and is consistent with support provided to commercial clients in the normal course of business. Facebook representatives advise political advertisers on Facebook, as they would with other, non-political managed accounts. We have a compliance team that trains our sales representatives to comply with all federal election law requirements in this area.

While no one from Facebook was assigned full-time to the Trump campaign, Facebook employees did interact with Cambridge Analytica employees. While our investigation is ongoing, our review indicates that Facebook employees did not identify any issues involving the improper use of Facebook data in the course of their interactions with Cambridge Analytica during the 2016 US Presidential campaign.

Election Integrity: In the run-up to the 2016 elections, we were focused on the kinds of cybersecurity attacks typically used by nation states, for example phishing and malware attacks. And we were too slow to spot information operations interference. Since then, we've made important changes to prevent bad actors from using misinformation to undermine the democratic process. This will never be a solved problem because we're up against determined, creative and well-funded adversaries. But we are making steady progress. Here is a list of the 10 most important changes we have made:

- **Ads transparency.** Advertising should be transparent: users should be able to see all the ads an advertiser is currently running on Facebook, Instagram and Messenger. And for ads with political content, we've created an archive that will hold ads with political content for seven years—including information about ad impressions and spend, as well as demographic data such as age, gender and location. People in Canada and Ireland have already been able to see all the ads that a Page is running on Facebook—and we've launched this globally.

- **Verification and labeling.** Every advertiser will now need to confirm their ID and location before being able to run any ads with political content in the US. All ads with political content will also clearly state who paid for them.

- **Updating targeting.** We want ads on Facebook to be safe and civil. We thoroughly review the targeting criteria advertisers can use to ensure they are consistent with our principles. As a result, we removed nearly one-third of the targeting segments used by the IRA. We continue to allow some criteria that people may find controversial. But we do see businesses marketing things like historical books, documentaries or television shows using them in legitimate ways.

- **Better technology.** Over the past year, we've gotten increasingly better at finding and disabling fake accounts. We now block millions of fake accounts each day as people try to create them—and before they've done any harm. This is thanks to improvements in machine learning and artificial intelligence, which can proactively identify suspicious behavior at a scale that was not possible before—without needing to look at the content itself.

- **Action to tackle fake news.** We are working hard to stop the spread of false news. We work with third-party fact-checking organizations to limit the spread of articles rated false. To reduce the spread of false news, we remove fake accounts and disrupt economic incentives for traffickers of misinformation. We also use various signals, including feedback from our community, to identify potential false news. In countries where we have partnerships with independent third-party fact-checkers, stories rated as false by those fact-checkers are shown lower in News Feed. If Pages or domains repeatedly create or share misinformation, we significantly reduce their distribution and remove their advertising rights. We also want to empower people to decide for themselves what to read, trust, and share. We promote news literacy and work to inform people with more context. For example, if third-party fact-checkers write articles about a news story, we show them immediately below the story in the Related Articles unit. We also notify people and Page Admins if they try to share a story, or have shared one in the past, that's

been determined to be false. In addition to our own efforts, we're learning from academics, scaling our partnerships with third-party fact-checkers and talking to other organizations about how we can work together.

A key focus is working to disrupt the economics of fake news. For example, preventing the creation of fake accounts that spread it, banning sites that engage in this behavior from using our ad products, and demoting articles found to be false by fact checkers in News Feed—causing it to lose 80% of its traffic. We now work with independent fact checkers in the US, France, Germany, Ireland, the Netherlands, Italy, Mexico, Colombia, India, Indonesia and the Philippines with plans to scale to more countries in the coming months.

- **Significant investments in security.** We're doubling the number of people working on safety and security from 10,000 last year to over 20,000 this year. We expect these investments to impact our profitability. But the safety of people using Facebook needs to come before profit.

- **Industry collaboration.** Recently, we joined 34 global tech and security companies in signing a TechAccord pact to help improve security for everyone.

- **Information sharing and reporting channels.** In the 2017 German elections, we worked closely with the authorities there, including the Federal Office for Information Security (BSI). This gave them a dedicated reporting channel for security issues related to the federal elections.

- **Tracking 40+ elections.** In recent months, we've started to deploy new tools and teams to proactively identify threats in the run-up to specific elections. We first tested this effort during the Alabama Senate election, and plan to continue these efforts for elections around the globe, including the US midterms. Last year we used public service announcements to help inform people about fake news in 21 separate countries, including in advance of French, Kenyan and German elections.

- **Action against the Russia-based IRA.** In April, we removed 70 Facebook and 65 Instagram accounts—as well as 138 Facebook Pages—controlled by the IRA primarily targeted either at people living in Russia or Russian-speakers around the world including from neighboring countries like Azerbaijan, Uzbekistan and Ukraine. The IRA has repeatedly used complex networks of inauthentic accounts to deceive and manipulate people in the US, Europe and Russia—and we don't want them on Facebook anywhere in the world.

327. FB now understands the nefarious activity of the 2016 election, but bad actors are always one step ahead. What are you doing to stay in front of any such activity and finding out before it's too late?

We want our platform to be a place where people can have authentic conversations about elections and other political topics. We believe this kind of engagement promotes democracy, but we know that there are actors working to interfere with those conversations and undermine our

elections. We are already taking steps to proactively prevent election interference and we are strengthening these protections going forward.

Engagement with campaigns: We want all candidates, groups, and voters to use our platform to engage in elections. We want it to be easy for people to find, follow, and contact their elected representatives—and those running to represent them. That's why, for candidates across the political spectrum, Facebook offers the same levels of support in key moments to help campaigns understand how best to use the platform. Both the Obama and Romney campaigns had access to the same tools, and no campaign received any special treatment from Facebook. Likewise, we offered identical support to both the Trump and Clinton campaigns, and had teams assigned to both. Everyone had access to the same tools, which are the same tools that every campaign is offered, and is consistent with support provided to commercial clients in the normal course of business. Facebook representatives advise political advertisers on Facebook, as they would with other, non-political managed accounts. We have a compliance team that trains our sales representatives to comply with all federal election law requirements in this area.

While no one from Facebook was assigned full-time to the Trump campaign, Facebook employees did interact with Cambridge Analytica employees. While our investigation is ongoing, our review indicates that Facebook employees did not identify any issues involving the improper use of Facebook data in the course of their interactions with Cambridge Analytica during the 2016 US Presidential campaign.

Election Integrity: In the run-up to the 2016 elections, we were focused on the kinds of cybersecurity attacks typically used by nation states, for example phishing and malware attacks. And we were too slow to spot information operations interference. Since then, we've made important changes to prevent bad actors from using misinformation to undermine the democratic process. This will never be a solved problem because we're up against determined, creative and well-funded adversaries. But we are making steady progress. Here is a list of the 10 most important changes we have made:

- **Ads transparency.** Advertising should be transparent: users should be able to see all the ads an advertiser is currently running on Facebook, Instagram and Messenger. And for ads with political content, we've created an archive that will hold ads with political content for seven years—including information about ad impressions and spend, as well as demographic data such as age, gender and location. People in Canada and Ireland have already been able to see all the ads that a Page is running on Facebook—and we've launched this globally.

- **Verification and labeling.** Every advertiser will now need to confirm their ID and location before being able to run any ads with political content in the US. All ads with political content will also clearly state who paid for them.

- **Updating targeting.** We want ads on Facebook to be safe and civil. We thoroughly review the targeting criteria advertisers can use to ensure they are consistent with our principles. As a result, we removed nearly one-third of the targeting segments used by the IRA. We continue to allow some criteria that people may find controversial. But we do

see businesses marketing things like historical books, documentaries or television shows using them in legitimate ways.

- **Better technology.** Over the past year, we've gotten increasingly better at finding and disabling fake accounts. We now block millions of fake accounts each day as people try to create them—and before they've done any harm. This is thanks to improvements in machine learning and artificial intelligence, which can proactively identify suspicious behavior at a scale that was not possible before—without needing to look at the content itself.

- **Action to tackle fake news.** We are working hard to stop the spread of false news. We work with third-party fact-checking organizations to limit the spread of articles rated false. To reduce the spread of false news, we remove fake accounts and disrupt economic incentives for traffickers of misinformation. We also use various signals, including feedback from our community, to identify potential false news. In countries where we have partnerships with independent third-party fact-checkers, stories rated as false by those fact-checkers are shown lower in News Feed. If Pages or domains repeatedly create or share misinformation, we significantly reduce their distribution and remove their advertising rights. We also want to empower people to decide for themselves what to read, trust, and share. We promote news literacy and work to inform people with more context. For example, if third-party fact-checkers write articles about a news story, we show them immediately below the story in the Related Articles unit. We also notify people and Page Admins if they try to share a story, or have shared one in the past, that's been determined to be false. In addition to our own efforts, we're learning from academics, scaling our partnerships with third-party fact-checkers and talking to other organizations about how we can work together.

  A key focus is working to disrupt the economics of fake news. For example, preventing the creation of fake accounts that spread it, banning sites that engage in this behavior from using our ad products, and demoting articles found to be false by fact checkers in News Feed—causing it to lose 80% of its traffic. We now work with independent fact checkers in the US, France, Germany, Ireland, the Netherlands, Italy, Mexico, Colombia, India, Indonesia and the Philippines with plans to scale to more countries in the coming months.

- **Significant investments in security.** We're doubling the number of people working on safety and security from 10,000 last year to over 20,000 this year. We expect these investments to impact our profitability. But the safety of people using Facebook needs to come before profit.

- **Industry collaboration.** Recently, we joined 34 global tech and security companies in signing a TechAccord pact to help improve security for everyone.

- **Information sharing and reporting channels.** In the 2017 German elections, we worked closely with the authorities there, including the Federal Office for Information Security (BSI). This gave them a dedicated reporting channel for security issues related to the federal elections.

- **Tracking 40+ elections.** In recent months, we've started to deploy new tools and teams to proactively identify threats in the run-up to specific elections. We first tested this effort during the Alabama Senate election, and plan to continue these efforts for elections around the globe, including the US midterms. Last year we used public service announcements to help inform people about fake news in 21 separate countries, including in advance of French, Kenyan and German elections.

- **Action against the Russia-based IRA.** In April, we removed 70 Facebook and 65 Instagram accounts—as well as 138 Facebook Pages—controlled by the IRA primarily targeted either at people living in Russia or Russian-speakers around the world including from neighboring countries like Azerbaijan, Uzbekistan and Ukraine. The IRA has repeatedly used complex networks of inauthentic accounts to deceive and manipulate people in the US, Europe and Russia—and we don't want them on Facebook anywhere in the world.

328. How can you, on one hand, tell advertisers that your platform is an effective use of marketing dollars, while on the other, try to tell the American people that illegally-run election ads placed by foreign nationals wouldn't have made a difference?

For years, we had been aware of other types of activity that appeared to come from Russian sources—largely traditional security threats such as attacking people's accounts or using social media platforms to spread stolen information. What we saw early in the 2016 campaign cycle followed this pattern. Our security team that focuses on threat intelligence—which investigates advanced security threats as part of our overall information security organization—was, from the outset, alert to the possibility of Russian activity. In several instances before November 8, 2016, this team detected and mitigated threats from actors with ties to Russia and reported them to US law enforcement officials. This included activity from a cluster of accounts we had assessed to belong to a group (APT28) that the US government has publicly linked to Russian military intelligence services. This activity, which was aimed at employees of major US political parties, fell into the normal categories of offensive cyber activities we monitor for. We warned the targets who were at highest risk, and were later in contact with law enforcement authorities about this activity.

Later in the summer we also started to see a new kind of behavior from APT28-related accounts—namely, the creation of fake personas that were then used to seed stolen information to journalists. These fake personas were organized under the banner of an organization that called itself DC Leaks. This activity violated our policies, and we removed the DC Leaks accounts.

Facebook learned from press accounts and statements by congressional leaders that Russian actors might have tried to interfere in the 2016 election by exploiting Facebook's ad tools. This is not something we had seen before, and so we started an investigation. We found that fake accounts associated with the IRA tried to influence the election.

This will never be a solved problem because we're up against determined, creative and well-funded adversaries. But we are making steady progress in preventing bad actors from using misinformation to undermine the democratic process, such as: increased ad transparency,

advertiser verification and labeling, updating targeting criteria, better technological efforts to find and disable fake accounts, third-party fact checking to stop the spread of false news, doubling the number of people working on safety and security, greater industry collaboration, increased information sharing and reporting channels, proactive identification of election threats, and specific action against the Russia-based IRA.

We will continue to work with the government, and across the tech industry and civil society, to address this important national security matter so that we can do our part to prevent similar abuse from happening again.

329. How do you plan to protect your platform from future exploit by foreign entities?

For years, we had been aware of other types of activity that appeared to come from Russian sources—largely traditional security threats such as attacking people's accounts or using social media platforms to spread stolen information. What we saw early in the 2016 campaign cycle followed this pattern. Our security team that focuses on threat intelligence—which investigates advanced security threats as part of our overall information security organization—was, from the outset, alert to the possibility of Russian activity. In several instances before November 8, 2016, this team detected and mitigated threats from actors with ties to Russia and reported them to US law enforcement officials. This included activity from a cluster of accounts we had assessed to belong to a group (APT28) that the US government has publicly linked to Russian military intelligence services. This activity, which was aimed at employees of major US political parties, fell into the normal categories of offensive cyber activities we monitor for. We warned the targets who were at highest risk, and were later in contact with law enforcement authorities about this activity.

Later in the summer we also started to see a new kind of behavior from APT28-related accounts—namely, the creation of fake personas that were then used to seed stolen information to journalists. These fake personas were organized under the banner of an organization that called itself DC Leaks. This activity violated our policies, and we removed the DC Leaks accounts.

Facebook learned from press accounts and statements by congressional leaders that Russian actors might have tried to interfere in the 2016 election by exploiting Facebook's ad tools. This is not something we had seen before, and so we started an investigation. We found that fake accounts associated with the IRA tried to influence the election.

This will never be a solved problem because we're up against determined, creative and well-funded adversaries. But we are making steady progress in preventing bad actors from using misinformation to undermine the democratic process, such as: increased ad transparency, advertiser verification and labeling, updating targeting criteria, better technological efforts to find and disable fake accounts, third-party fact checking to stop the spread of false news, doubling the number of people working on safety and security, greater industry collaboration, increased information sharing and reporting channels, proactive identification of election threats, and specific action against the Russia-based IRA.

We will continue to work with the government, and across the tech industry and civil society, to address this important national security matter so that we can do our part to prevent similar abuse from happening again.

330. How to control untruths via Facebook

We want Facebook to be a place where people can discover more news, information, and perspectives, and we are working to build products that help to that. Through our News Feed algorithm, we also work hard to actively reduce the distribution of clickbait, sensationalism, and misinformation, on the one hand, and to boost news and information from sources that are trusted, informative, and local, on the other hand.
We are focusing on four different strategies to address misinformation:

- **Strengthening enforcement of our authenticity policies.** We are investing heavily in new technology and hiring thousands more people to tackle the problem of inauthenticity on the platform. Fake accounts are often associated with false news, so this is an area that will have a huge impact on curbing the spread of inaccurate information.

- **Finding industry solutions.** All of us—from tech companies and media companies to newsrooms and classrooms—must work together to find industry solutions to strengthen the online news ecosystem and our own digital literacy. That's why we're collaborating with others who operate in this space. Last January, we announced The Facebook Journalism Project, an initiative that seeks to establish stronger ties between Facebook and the news industry. The project is focused on developing news products, providing training and tools for journalists, and working with publishers and educators on how we can equip people with the knowledge they need to be informed readers in the digital age. Since launching the Journalism Project, we've met with more than 2,600 publishers around the world to understand how they use our products and how we can make improvements to better support their needs.

- **Disrupting economic incentives.** When it comes to fighting false news, we've found that a lot of it is financially motivated. So, one of the most effective approaches is removing the economic incentives for those who traffic in inaccurate information. We've done things like block ads from pages that repeatedly share false news and significantly limit the distribution of web pages that deliver low quality web experiences.

- **Building new products.** We believe it's important to amplify the good effects of social media and mitigate the bad—to contribute to the diversity of ideas, information, and view points, while strengthening our common understanding.

    - We believe giving people more context can help them decide what to trust and what to share. The third-party fact-checking program we have developed uses reports from our community, along with other signals, to send stories to accredited third-party fact checking organizations. If the fact checking organizations identify a story as fake, we will suggest related articles in News Feed to show people different points of view, including information from fact checkers. Stories that have been disputed may also appear lower in News Feed.

Our own data analytics show that a false rating from one of our fact checking partners reduces future impressions on Facebook by 80 percent.

- We're also testing Article Context as a way of giving people more information about the material they're reading on Facebook. Since we launched this test, some of the articles people see in News Feed will feature an "i" icon that allows them to access more information at the tap of a button. The information we surface is pulled from across the internet, and includes things like the publisher's Wikipedia entry, trending articles or related articles about the topic, and information about how the article is being shared on Facebook. In some cases, if that information is unavailable, we will let people know since that can also be helpful context.

331. What is FB doing to trace how the hacked info is being used for purposes other than political targeting?

For years, we had been aware of other types of activity that appeared to come from Russian sources—largely traditional security threats such as attacking people's accounts or using social media platforms to spread stolen information. What we saw early in the 2016 campaign cycle followed this pattern. Our security team that focuses on threat intelligence—which investigates advanced security threats as part of our overall information security organization—was, from the outset, alert to the possibility of Russian activity. In several instances before November 8, 2016, this team detected and mitigated threats from actors with ties to Russia and reported them to US law enforcement officials. This included activity from a cluster of accounts we had assessed to belong to a group (APT28) that the US government has publicly linked to Russian military intelligence services. This activity, which was aimed at employees of major US political parties, fell into the normal categories of offensive cyber activities we monitor for. We warned the targets who were at highest risk, and were later in contact with law enforcement authorities about this activity.

Later in the summer we also started to see a new kind of behavior from APT28-related accounts—namely, the creation of fake personas that were then used to seed stolen information to journalists. These fake personas were organized under the banner of an organization that called itself DC Leaks. This activity violated our policies, and we removed the DC Leaks accounts.

Facebook learned from press accounts and statements by congressional leaders that Russian actors might have tried to interfere in the 2016 election by exploiting Facebook's ad tools. This is not something we had seen before, and so we started an investigation. We found that fake accounts associated with the IRA tried to influence the election.

This will never be a solved problem because we're up against determined, creative and well-funded adversaries. But we are making steady progress in preventing bad actors from using misinformation to undermine the democratic process, such as: increased ad transparency, advertiser verification and labeling, updating targeting criteria, better technological efforts to find and disable fake accounts, third-party fact checking to stop the spread of false news, doubling the number of people working on safety and security, greater industry collaboration,

increased information sharing and reporting channels, proactive identification of election threats, and specific action against the Russia-based IRA.

We will continue to work with the government, and across the tech industry and civil society, to address this important national security matter so that we can do our part to prevent similar abuse from happening again.

332. How would you verify not only the legitimacy of a post and also prevent the spreading of hatred?

We want Facebook to be a place where people can discover more news, information, and perspectives, and we are working to build products that help to that. Through our News Feed algorithm, we also work hard to actively reduce the distribution of clickbait, sensationalism, and misinformation, on the one hand, and to boost news and information from sources that are trusted, informative, and local, on the other hand.
We are focusing on four different strategies to address misinformation:

- **Strengthening enforcement of our authenticity policies.** We are investing heavily in new technology and hiring thousands more people to tackle the problem of inauthenticity on the platform. Fake accounts are often associated with false news, so this is an area that will have a huge impact on curbing the spread of inaccurate information.

- **Finding industry solutions.** All of us—from tech companies and media companies to newsrooms and classrooms—must work together to find industry solutions to strengthen the online news ecosystem and our own digital literacy. That's why we're collaborating with others who operate in this space. Last January, we announced The Facebook Journalism Project, an initiative that seeks to establish stronger ties between Facebook and the news industry. The project is focused on developing news products, providing training and tools for journalists, and working with publishers and educators on how we can equip people with the knowledge they need to be informed readers in the digital age. Since launching the Journalism Project, we've met with more than 2,600 publishers around the world to understand how they use our products and how we can make improvements to better support their needs.

- **Disrupting economic incentives.** When it comes to fighting false news, we've found that a lot of it is financially motivated. So, one of the most effective approaches is removing the economic incentives for those who traffic in inaccurate information. We've done things like block ads from pages that repeatedly share false news and significantly limit the distribution of web pages that deliver low quality web experiences.

- **Building new products.** We believe it's important to amplify the good effects of social media and mitigate the bad—to contribute to the diversity of ideas, information, and view points, while strengthening our common understanding.

    - We believe giving people more context can help them decide what to trust and what to share. The third-party fact-checking program we have developed uses reports from our community, along with other signals, to send stories to accredited third-party fact checking organizations. If the fact checking

organizations identify a story as fake, we will suggest related articles in News Feed to show people different points of view, including information from fact checkers. Stories that have been disputed may also appear lower in News Feed. Our own data analytics show that a false rating from one of our fact checking partners reduces future impressions on Facebook by 80 percent.

- We're also testing Article Context as a way of giving people more information about the material they're reading on Facebook. Since we launched this test, some of the articles people see in News Feed will feature an "i" icon that allows them to access more information at the tap of a button. The information we surface is pulled from across the internet, and includes things like the publisher's Wikipedia entry, trending articles or related articles about the topic, and information about how the article is being shared on Facebook. In some cases, if that information is unavailable, we will let people know since that can also be helpful context.

333. What specific actions is Facebook taking to prevent false news stories and malicious meddling in the 2018 election?

We want Facebook to be a place where people can discover more news, information, and perspectives, and we are working to build products that help to that. Through our News Feed algorithm, we also work hard to actively reduce the distribution of clickbait, sensationalism, and misinformation, on the one hand, and to boost news and information from sources that are trusted, informative, and local, on the other hand.

We are focusing on four different strategies to address misinformation:

- **Strengthening enforcement of our authenticity policies.** We are investing heavily in new technology and hiring thousands more people to tackle the problem of inauthenticity on the platform. Fake accounts are often associated with false news, so this is an area that will have a huge impact on curbing the spread of inaccurate information.

- **Finding industry solutions.** All of us—from tech companies and media companies to newsrooms and classrooms—must work together to find industry solutions to strengthen the online news ecosystem and our own digital literacy. That's why we're collaborating with others who operate in this space. Last January, we announced The Facebook Journalism Project, an initiative that seeks to establish stronger ties between Facebook and the news industry. The project is focused on developing news products, providing training and tools for journalists, and working with publishers and educators on how we can equip people with the knowledge they need to be informed readers in the digital age. Since launching the Journalism Project, we've met with more than 2,600 publishers around the world to understand how they use our products and how we can make improvements to better support their needs.

- **Disrupting economic incentives.** When it comes to fighting false news, we've found that a lot of it is financially motivated. So, one of the most effective approaches is removing the economic incentives for those who traffic in inaccurate information. We've done

things like block ads from pages that repeatedly share false news and significantly limit the distribution of web pages that deliver low quality web experiences.

- **Building new products.** We believe it's important to amplify the good effects of social media and mitigate the bad—to contribute to the diversity of ideas, information, and view points, while strengthening our common understanding.

    - We believe giving people more context can help them decide what to trust and what to share. The third-party fact-checking program we have developed uses reports from our community, along with other signals, to send stories to accredited third-party fact checking organizations. If the fact checking organizations identify a story as fake, we will suggest related articles in News Feed to show people different points of view, including information from fact checkers. Stories that have been disputed may also appear lower in News Feed. Our own data analytics show that a false rating from one of our fact checking partners reduces future impressions on Facebook by 80 percent.

    - We're also testing Article Context as a way of giving people more information about the material they're reading on Facebook. Since we launched this test, some of the articles people see in News Feed will feature an "i" icon that allows them to access more information at the tap of a button. The information we surface is pulled from across the internet, and includes things like the publisher's Wikipedia entry, trending articles or related articles about the topic, and information about how the article is being shared on Facebook. In some cases, if that information is unavailable, we will let people know since that can also be helpful context.

334. Using AI or conventional methods, what steps will you take to detect/eliminate trolling and misinformation from foreign/domestic entities?

For years, we had been aware of other types of activity that appeared to come from Russian sources—largely traditional security threats such as attacking people's accounts or using social media platforms to spread stolen information. What we saw early in the 2016 campaign cycle followed this pattern. Our security team that focuses on threat intelligence—which investigates advanced security threats as part of our overall information security organization—was, from the outset, alert to the possibility of Russian activity. In several instances before November 8, 2016, this team detected and mitigated threats from actors with ties to Russia and reported them to US law enforcement officials. This included activity from a cluster of accounts we had assessed to belong to a group (APT28) that the US government has publicly linked to Russian military intelligence services. This activity, which was aimed at employees of major US political parties, fell into the normal categories of offensive cyber activities we monitor for. We warned the targets who were at highest risk, and were later in contact with law enforcement authorities about this activity.

Later in the summer we also started to see a new kind of behavior from APT28-related accounts—namely, the creation of fake personas that were then used to seed stolen information to journalists. These fake personas were organized under the banner of an organization that

called itself DC Leaks. This activity violated our policies, and we removed the DC Leaks accounts.

Facebook learned from press accounts and statements by congressional leaders that Russian actors might have tried to interfere in the 2016 election by exploiting Facebook's ad tools. This is not something we had seen before, and so we started an investigation. We found that fake accounts associated with the IRA tried to influence the election.

This will never be a solved problem because we're up against determined, creative and well-funded adversaries. But we are making steady progress in preventing bad actors from using misinformation to undermine the democratic process, such as: increased ad transparency, advertiser verification and labeling, updating targeting criteria, better technological efforts to find and disable fake accounts, third-party fact checking to stop the spread of false news, doubling the number of people working on safety and security, greater industry collaboration, increased information sharing and reporting channels, proactive identification of election threats, and specific action against the Russia-based IRA.

We will continue to work with the government, and across the tech industry and civil society, to address this important national security matter so that we can do our part to prevent similar abuse from happening again.

335. Cambridge Analytics reportedly used Facebook data to target Brexit voters in 2016. Why didn't this manipulated outcome (done without Facebook users' permission) get your attention before Trump did the same thing in the U.S. election? How can you guarantee that this will not happen again in 2018?

We want our platform to be a place where people can have authentic conversations about elections and other political topics. We believe this kind of engagement promotes democracy, but we know that there are actors working to interfere with those conversations and undermine our elections. We are already taking steps to proactively prevent election interference and we are strengthening these protections going forward.

Engagement with campaigns: We want all candidates, groups, and voters to use our platform to engage in elections. We want it to be easy for people to find, follow, and contact their elected representatives—and those running to represent them. That's why, for candidates across the political spectrum, Facebook offers the same levels of support in key moments to help campaigns understand how best to use the platform. Both the Obama and Romney campaigns had access to the same tools, and no campaign received any special treatment from Facebook. Likewise, we offered identical support to both the Trump and Clinton campaigns, and had teams assigned to both. Everyone had access to the same tools, which are the same tools that every campaign is offered, and is consistent with support provided to commercial clients in the normal course of business. Facebook representatives advise political advertisers on Facebook, as they would with other, non-political managed accounts. We have a compliance team that trains our sales representatives to comply with all federal election law requirements in this area.

While no one from Facebook was assigned full-time to the Trump campaign, Facebook employees did interact with Cambridge Analytica employees. While our investigation is

ongoing, our review indicates that Facebook employees did not identify any issues involving the improper use of Facebook data in the course of their interactions with Cambridge Analytica during the 2016 US Presidential campaign.

Election Integrity: In the run-up to the 2016 elections, we were focused on the kinds of cybersecurity attacks typically used by nation states, for example phishing and malware attacks. And we were too slow to spot information operations interference. Since then, we've made important changes to prevent bad actors from using misinformation to undermine the democratic process. This will never be a solved problem because we're up against determined, creative and well-funded adversaries. But we are making steady progress. Here is a list of the 10 most important changes we have made:

- **Ads transparency.** Advertising should be transparent: users should be able to see all the ads an advertiser is currently running on Facebook, Instagram and Messenger. And for ads with political content, we've created an archive that will hold ads with political content for seven years—including information about ad impressions and spend, as well as demographic data such as age, gender and location. People in Canada and Ireland have already been able to see all the ads that a Page is running on Facebook—and we've launched this globally.

- **Verification and labeling.** Every advertiser will now need to confirm their ID and location before being able to run any ads with political content in the US. All ads with political content will also clearly state who paid for them.

- **Updating targeting.** We want ads on Facebook to be safe and civil. We thoroughly review the targeting criteria advertisers can use to ensure they are consistent with our principles. As a result, we removed nearly one-third of the targeting segments used by the IRA. We continue to allow some criteria that people may find controversial. But we do see businesses marketing things like historical books, documentaries or television shows using them in legitimate ways.

- **Better technology.** Over the past year, we've gotten increasingly better at finding and disabling fake accounts. We now block millions of fake accounts each day as people try to create them—and before they've done any harm. This is thanks to improvements in machine learning and artificial intelligence, which can proactively identify suspicious behavior at a scale that was not possible before—without needing to look at the content itself.

- **Action to tackle fake news.** We are working hard to stop the spread of false news. We work with third-party fact-checking organizations to limit the spread of articles rated false. To reduce the spread of false news, we remove fake accounts and disrupt economic incentives for traffickers of misinformation. We also use various signals, including feedback from our community, to identify potential false news. In countries where we have partnerships with independent third-party fact-checkers, stories rated as false by those fact-checkers are shown lower in News Feed. If Pages or domains repeatedly create or share misinformation, we significantly reduce their distribution and remove their advertising rights. We also want to empower people to decide for themselves what to

read, trust, and share. We promote news literacy and work to inform people with more context. For example, if third-party fact-checkers write articles about a news story, we show them immediately below the story in the Related Articles unit. We also notify people and Page Admins if they try to share a story, or have shared one in the past, that's been determined to be false. In addition to our own efforts, we're learning from academics, scaling our partnerships with third-party fact-checkers and talking to other organizations about how we can work together.

A key focus is working to disrupt the economics of fake news. For example, preventing the creation of fake accounts that spread it, banning sites that engage in this behavior from using our ad products, and demoting articles found to be false by fact checkers in News Feed—causing it to lose 80% of its traffic. We now work with independent fact checkers in the US, France, Germany, Ireland, the Netherlands, Italy, Mexico, Colombia, India, Indonesia and the Philippines with plans to scale to more countries in the coming months.

- **Significant investments in security.** We're doubling the number of people working on safety and security from 10,000 last year to over 20,000 this year. We expect these investments to impact our profitability. But the safety of people using Facebook needs to come before profit.

- **Industry collaboration.** Recently, we joined 34 global tech and security companies in signing a TechAccord pact to help improve security for everyone.

- **Information sharing and reporting channels.** In the 2017 German elections, we worked closely with the authorities there, including the Federal Office for Information Security (BSI). This gave them a dedicated reporting channel for security issues related to the federal elections.

- **Tracking 40+ elections.** In recent months, we've started to deploy new tools and teams to proactively identify threats in the run-up to specific elections. We first tested this effort during the Alabama Senate election, and plan to continue these efforts for elections around the globe, including the US midterms. Last year we used public service announcements to help inform people about fake news in 21 separate countries, including in advance of French, Kenyan and German elections.

- **Action against the Russia-based IRA.** In April, we removed 70 Facebook and 65 Instagram accounts—as well as 138 Facebook Pages—controlled by the IRA primarily targeted either at people living in Russia or Russian-speakers around the world including from neighboring countries like Azerbaijan, Uzbekistan and Ukraine. The IRA has repeatedly used complex networks of inauthentic accounts to deceive and manipulate people in the US, Europe and Russia—and we don't want them on Facebook anywhere in the world.

336. Explain, without excuses, the wide variance between your statements and real events with Russian uses of FB.

For years, we had been aware of other types of activity that appeared to come from Russian sources—largely traditional security threats such as attacking people's accounts or using social media platforms to spread stolen information. What we saw early in the 2016 campaign cycle followed this pattern. Our security team that focuses on threat intelligence—which investigates advanced security threats as part of our overall information security organization—was, from the outset, alert to the possibility of Russian activity. In several instances before November 8, 2016, this team detected and mitigated threats from actors with ties to Russia and reported them to US law enforcement officials. This included activity from a cluster of accounts we had assessed to belong to a group (APT28) that the US government has publicly linked to Russian military intelligence services. This activity, which was aimed at employees of major US political parties, fell into the normal categories of offensive cyber activities we monitor for. We warned the targets who were at highest risk, and were later in contact with law enforcement authorities about this activity.

Later in the summer we also started to see a new kind of behavior from APT28-related accounts—namely, the creation of fake personas that were then used to seed stolen information to journalists. These fake personas were organized under the banner of an organization that called itself DC Leaks. This activity violated our policies, and we removed the DC Leaks accounts.

Facebook learned from press accounts and statements by congressional leaders that Russian actors might have tried to interfere in the 2016 election by exploiting Facebook's ad tools. This is not something we had seen before, and so we started an investigation. We found that fake accounts associated with the IRA tried to influence the election.

This will never be a solved problem because we're up against determined, creative and well-funded adversaries. But we are making steady progress in preventing bad actors from using misinformation to undermine the democratic process, such as: increased ad transparency, advertiser verification and labeling, updating targeting criteria, better technological efforts to find and disable fake accounts, third-party fact checking to stop the spread of false news, doubling the number of people working on safety and security, greater industry collaboration, increased information sharing and reporting channels, proactive identification of election threats, and specific action against the Russia-based IRA.

We will continue to work with the government, and across the tech industry and civil society, to address this important national security matter so that we can do our part to prevent similar abuse from happening again.

337. In your estimation, how can we, as a country, protect ourselves from misinformation that undermines our democracy and tears our society apart? What do you see as social media's role in ensuring that it serves all of our best interests and is not a tool for those who might want to do us harm or sow the seeds of discontent?

We want Facebook to be a place where people can discover more news, information, and perspectives, and we are working to build products that help to that. Through our News Feed algorithm, we also work hard to actively reduce the distribution of clickbait, sensationalism, and

misinformation, on the one hand, and to boost news and information from sources that are trusted, informative, and local, on the other hand. We are focusing on four different strategies to address misinformation:

- **Strengthening enforcement of our authenticity policies.** We are investing heavily in new technology and hiring thousands more people to tackle the problem of inauthenticity on the platform. Fake accounts are often associated with false news, so this is an area that will have a huge impact on curbing the spread of inaccurate information.

- **Finding industry solutions.** All of us—from tech companies and media companies to newsrooms and classrooms—must work together to find industry solutions to strengthen the online news ecosystem and our own digital literacy. That's why we're collaborating with others who operate in this space. Last January, we announced The Facebook Journalism Project, an initiative that seeks to establish stronger ties between Facebook and the news industry. The project is focused on developing news products, providing training and tools for journalists, and working with publishers and educators on how we can equip people with the knowledge they need to be informed readers in the digital age. Since launching the Journalism Project, we've met with more than 2,600 publishers around the world to understand how they use our products and how we can make improvements to better support their needs.

- **Disrupting economic incentives.** When it comes to fighting false news, we've found that a lot of it is financially motivated. So, one of the most effective approaches is removing the economic incentives for those who traffic in inaccurate information. We've done things like block ads from pages that repeatedly share false news and significantly limit the distribution of web pages that deliver low quality web experiences.

- **Building new products.** We believe it's important to amplify the good effects of social media and mitigate the bad—to contribute to the diversity of ideas, information, and view points, while strengthening our common understanding.

    - We believe giving people more context can help them decide what to trust and what to share. The third-party fact-checking program we have developed uses reports from our community, along with other signals, to send stories to accredited third-party fact checking organizations. If the fact checking organizations identify a story as fake, we will suggest related articles in News Feed to show people different points of view, including information from fact checkers. Stories that have been disputed may also appear lower in News Feed. Our own data analytics show that a false rating from one of our fact checking partners reduces future impressions on Facebook by 80 percent.

    - We're also testing Article Context as a way of giving people more information about the material they're reading on Facebook. Since we launched this test, some of the articles people see in News Feed will feature an "i" icon that allows them to access more information at the tap of a button. The information we surface is pulled from across the internet, and includes things like the publisher's Wikipedia entry, trending articles or related articles about the topic, and information about

how the article is being shared on Facebook. In some cases, if that information is unavailable, we will let people know since that can also be helpful context.

338. Will you pledge to be transparent about foreign powers trying to use Facebook to subvert elections?

For years, we had been aware of other types of activity that appeared to come from Russian sources—largely traditional security threats such as attacking people's accounts or using social media platforms to spread stolen information. What we saw early in the 2016 campaign cycle followed this pattern. Our security team that focuses on threat intelligence—which investigates advanced security threats as part of our overall information security organization—was, from the outset, alert to the possibility of Russian activity. In several instances before November 8, 2016, this team detected and mitigated threats from actors with ties to Russia and reported them to US law enforcement officials. This included activity from a cluster of accounts we had assessed to belong to a group (APT28) that the US government has publicly linked to Russian military intelligence services. This activity, which was aimed at employees of major US political parties, fell into the normal categories of offensive cyber activities we monitor for. We warned the targets who were at highest risk, and were later in contact with law enforcement authorities about this activity.

Later in the summer we also started to see a new kind of behavior from APT28-related accounts—namely, the creation of fake personas that were then used to seed stolen information to journalists. These fake personas were organized under the banner of an organization that called itself DC Leaks. This activity violated our policies, and we removed the DC Leaks accounts.

Facebook learned from press accounts and statements by congressional leaders that Russian actors might have tried to interfere in the 2016 election by exploiting Facebook's ad tools. This is not something we had seen before, and so we started an investigation. We found that fake accounts associated with the IRA tried to influence the election.

This will never be a solved problem because we're up against determined, creative and well-funded adversaries. But we are making steady progress in preventing bad actors from using misinformation to undermine the democratic process, such as: increased ad transparency, advertiser verification and labeling, updating targeting criteria, better technological efforts to find and disable fake accounts, third-party fact checking to stop the spread of false news, doubling the number of people working on safety and security, greater industry collaboration, increased information sharing and reporting channels, proactive identification of election threats, and specific action against the Russia-based IRA.

We will continue to work with the government, and across the tech industry and civil society, to address this important national security matter so that we can do our part to prevent similar abuse from happening again.

339. What specific actions will you take to prevent foreign interference in US elections?

For years, we had been aware of other types of activity that appeared to come from Russian sources—largely traditional security threats such as attacking people's accounts or using

social media platforms to spread stolen information. What we saw early in the 2016 campaign cycle followed this pattern. Our security team that focuses on threat intelligence—which investigates advanced security threats as part of our overall information security organization—was, from the outset, alert to the possibility of Russian activity. In several instances before November 8, 2016, this team detected and mitigated threats from actors with ties to Russia and reported them to US law enforcement officials. This included activity from a cluster of accounts we had assessed to belong to a group (APT28) that the US government has publicly linked to Russian military intelligence services. This activity, which was aimed at employees of major US political parties, fell into the normal categories of offensive cyber activities we monitor for. We warned the targets who were at highest risk, and were later in contact with law enforcement authorities about this activity.

Later in the summer we also started to see a new kind of behavior from APT28-related accounts—namely, the creation of fake personas that were then used to seed stolen information to journalists. These fake personas were organized under the banner of an organization that called itself DC Leaks. This activity violated our policies, and we removed the DC Leaks accounts.

Facebook learned from press accounts and statements by congressional leaders that Russian actors might have tried to interfere in the 2016 election by exploiting Facebook's ad tools. This is not something we had seen before, and so we started an investigation. We found that fake accounts associated with the IRA tried to influence the election.

This will never be a solved problem because we're up against determined, creative and well-funded adversaries. But we are making steady progress in preventing bad actors from using misinformation to undermine the democratic process, such as: increased ad transparency, advertiser verification and labeling, updating targeting criteria, better technological efforts to find and disable fake accounts, third-party fact checking to stop the spread of false news, doubling the number of people working on safety and security, greater industry collaboration, increased information sharing and reporting channels, proactive identification of election threats, and specific action against the Russia-based IRA.

We will continue to work with the government, and across the tech industry and civil society, to address this important national security matter so that we can do our part to prevent similar abuse from happening again.

340. Mr. Zuckerberg, did Facebook provide user data to the Obama campaign in 2012?

We want our platform to be a place where people can have authentic conversations about elections and other political topics. We believe this kind of engagement promotes democracy, but we know that there are actors working to interfere with those conversations and undermine our elections. We are already taking steps to proactively prevent election interference and we are strengthening these protections going forward.

Engagement with campaigns: We want all candidates, groups, and voters to use our platform to engage in elections. We want it to be easy for people to find, follow, and contact their elected representatives—and those running to represent them. That's why, for candidates

across the political spectrum, Facebook offers the same levels of support in key moments to help campaigns understand how best to use the platform. Both the Obama and Romney campaigns had access to the same tools, and no campaign received any special treatment from Facebook. Likewise, we offered identical support to both the Trump and Clinton campaigns, and had teams assigned to both. Everyone had access to the same tools, which are the same tools that every campaign is offered, and is consistent with support provided to commercial clients in the normal course of business. Facebook representatives advise political advertisers on Facebook, as they would with other, non-political managed accounts. We have a compliance team that trains our sales representatives to comply with all federal election law requirements in this area.

While no one from Facebook was assigned full-time to the Trump campaign, Facebook employees did interact with Cambridge Analytica employees. While our investigation is ongoing, our review indicates that Facebook employees did not identify any issues involving the improper use of Facebook data in the course of their interactions with Cambridge Analytica during the 2016 US Presidential campaign.

Election Integrity: In the run-up to the 2016 elections, we were focused on the kinds of cybersecurity attacks typically used by nation states, for example phishing and malware attacks. And we were too slow to spot information operations interference. Since then, we've made important changes to prevent bad actors from using misinformation to undermine the democratic process. This will never be a solved problem because we're up against determined, creative and well-funded adversaries. But we are making steady progress. Here is a list of the 10 most important changes we have made:

- **Ads transparency.** Advertising should be transparent: users should be able to see all the ads an advertiser is currently running on Facebook, Instagram and Messenger. And for ads with political content, we've created an archive that will hold ads with political content for seven years—including information about ad impressions and spend, as well as demographic data such as age, gender and location. People in Canada and Ireland have already been able to see all the ads that a Page is running on Facebook—and we've launched this globally.

- **Verification and labeling.** Every advertiser will now need to confirm their ID and location before being able to run any ads with political content in the US. All ads with political content will also clearly state who paid for them.

- **Updating targeting.** We want ads on Facebook to be safe and civil. We thoroughly review the targeting criteria advertisers can use to ensure they are consistent with our principles. As a result, we removed nearly one-third of the targeting segments used by the IRA. We continue to allow some criteria that people may find controversial. But we do see businesses marketing things like historical books, documentaries or television shows using them in legitimate ways.

- **Better technology.** Over the past year, we've gotten increasingly better at finding and disabling fake accounts. We now block millions of fake accounts each day as people try to create them—and before they've done any harm. This is thanks to improvements in machine learning and artificial intelligence, which can proactively identify suspicious

behavior at a scale that was not possible before—without needing to look at the content itself.

- **Action to tackle fake news.** We are working hard to stop the spread of false news. We work with third-party fact-checking organizations to limit the spread of articles rated false. To reduce the spread of false news, we remove fake accounts and disrupt economic incentives for traffickers of misinformation. We also use various signals, including feedback from our community, to identify potential false news. In countries where we have partnerships with independent third-party fact-checkers, stories rated as false by those fact-checkers are shown lower in News Feed. If Pages or domains repeatedly create or share misinformation, we significantly reduce their distribution and remove their advertising rights. We also want to empower people to decide for themselves what to read, trust, and share. We promote news literacy and work to inform people with more context. For example, if third-party fact-checkers write articles about a news story, we show them immediately below the story in the Related Articles unit. We also notify people and Page Admins if they try to share a story, or have shared one in the past, that's been determined to be false. In addition to our own efforts, we're learning from academics, scaling our partnerships with third-party fact-checkers and talking to other organizations about how we can work together.

  A key focus is working to disrupt the economics of fake news. For example, preventing the creation of fake accounts that spread it, banning sites that engage in this behavior from using our ad products, and demoting articles found to be false by fact checkers in News Feed—causing it to lose 80% of its traffic. We now work with independent fact checkers in the US, France, Germany, Ireland, the Netherlands, Italy, Mexico, Colombia, India, Indonesia and the Philippines with plans to scale to more countries in the coming months.

- **Significant investments in security.** We're doubling the number of people working on safety and security from 10,000 last year to over 20,000 this year. We expect these investments to impact our profitability. But the safety of people using Facebook needs to come before profit.

- **Industry collaboration.** Recently, we joined 34 global tech and security companies in signing a TechAccord pact to help improve security for everyone.

- **Information sharing and reporting channels.** In the 2017 German elections, we worked closely with the authorities there, including the Federal Office for Information Security (BSI). This gave them a dedicated reporting channel for security issues related to the federal elections.

- **Tracking 40+ elections.** In recent months, we've started to deploy new tools and teams to proactively identify threats in the run-up to specific elections. We first tested this effort during the Alabama Senate election, and plan to continue these efforts for elections around the globe, including the US midterms. Last year we used public service announcements to help inform people about fake news in 21 separate countries, including in advance of French, Kenyan and German elections.

- **Action against the Russia-based IRA.** In April, we removed 70 Facebook and 65 Instagram accounts—as well as 138 Facebook Pages—controlled by the IRA primarily targeted either at people living in Russia or Russian-speakers around the world including from neighboring countries like Azerbaijan, Uzbekistan and Ukraine. The IRA has repeatedly used complex networks of inauthentic accounts to deceive and manipulate people in the US, Europe and Russia—and we don't want them on Facebook anywhere in the world.

341. How can we stop invisible Individually-targeted propaganda machines that seek to alter election results?

We want Facebook to be a place where people can discover more news, information, and perspectives, and we are working to build products that help to that. Through our News Feed algorithm, we also work hard to actively reduce the distribution of clickbait, sensationalism, and misinformation, on the one hand, and to boost news and information from sources that are trusted, informative, and local, on the other hand.
We are focusing on four different strategies to address misinformation:

- **Strengthening enforcement of our authenticity policies.** We are investing heavily in new technology and hiring thousands more people to tackle the problem of inauthenticity on the platform. Fake accounts are often associated with false news, so this is an area that will have a huge impact on curbing the spread of inaccurate information.

- **Finding industry solutions.** All of us—from tech companies and media companies to newsrooms and classrooms—must work together to find industry solutions to strengthen the online news ecosystem and our own digital literacy. That's why we're collaborating with others who operate in this space. Last January, we announced The Facebook Journalism Project, an initiative that seeks to establish stronger ties between Facebook and the news industry. The project is focused on developing news products, providing training and tools for journalists, and working with publishers and educators on how we can equip people with the knowledge they need to be informed readers in the digital age. Since launching the Journalism Project, we've met with more than 2,600 publishers around the world to understand how they use our products and how we can make improvements to better support their needs.

- **Disrupting economic incentives.** When it comes to fighting false news, we've found that a lot of it is financially motivated. So, one of the most effective approaches is removing the economic incentives for those who traffic in inaccurate information. We've done things like block ads from pages that repeatedly share false news and significantly limit the distribution of web pages that deliver low quality web experiences.

- **Building new products.** We believe it's important to amplify the good effects of social media and mitigate the bad—to contribute to the diversity of ideas, information, and view points, while strengthening our common understanding.

    - We believe giving people more context can help them decide what to trust and what to share. The third-party fact-checking program we have developed uses

reports from our community, along with other signals, to send stories to accredited third-party fact checking organizations. If the fact checking organizations identify a story as fake, we will suggest related articles in News Feed to show people different points of view, including information from fact checkers. Stories that have been disputed may also appear lower in News Feed. Our own data analytics show that a false rating from one of our fact checking partners reduces future impressions on Facebook by 80 percent.

- We're also testing Article Context as a way of giving people more information about the material they're reading on Facebook. Since we launched this test, some of the articles people see in News Feed will feature an "i" icon that allows them to access more information at the tap of a button. The information we surface is pulled from across the internet, and includes things like the publisher's Wikipedia entry, trending articles or related articles about the topic, and information about how the article is being shared on Facebook. In some cases, if that information is unavailable, we will let people know since that can also be helpful context.

342. Mr. Zuckerberg: Can you tailor Facebook's business model so it will not become an existential threat to American Democracy?

We want our platform to be a place where people can have authentic conversations about elections and other political topics. We believe this kind of engagement promotes democracy, but we know that there are actors working to interfere with those conversations and undermine our elections. We are already taking steps to proactively prevent election interference and we are strengthening these protections going forward.

Engagement with campaigns: We want all candidates, groups, and voters to use our platform to engage in elections. We want it to be easy for people to find, follow, and contact their elected representatives—and those running to represent them. That's why, for candidates across the political spectrum, Facebook offers the same levels of support in key moments to help campaigns understand how best to use the platform. Both the Obama and Romney campaigns had access to the same tools, and no campaign received any special treatment from Facebook. Likewise, we offered identical support to both the Trump and Clinton campaigns, and had teams assigned to both. Everyone had access to the same tools, which are the same tools that every campaign is offered, and is consistent with support provided to commercial clients in the normal course of business. Facebook representatives advise political advertisers on Facebook, as they would with other, non-political managed accounts. We have a compliance team that trains our sales representatives to comply with all federal election law requirements in this area.

While no one from Facebook was assigned full-time to the Trump campaign, Facebook employees did interact with Cambridge Analytica employees. While our investigation is ongoing, our review indicates that Facebook employees did not identify any issues involving the improper use of Facebook data in the course of their interactions with Cambridge Analytica during the 2016 US Presidential campaign.

Election Integrity: In the run-up to the 2016 elections, we were focused on the kinds of cybersecurity attacks typically used by nation states, for example phishing and malware attacks.

And we were too slow to spot information operations interference. Since then, we've made important changes to prevent bad actors from using misinformation to undermine the democratic process. This will never be a solved problem because we're up against determined, creative and well-funded adversaries. But we are making steady progress. Here is a list of the 10 most important changes we have made:

- **Ads transparency.** Advertising should be transparent: users should be able to see all the ads an advertiser is currently running on Facebook, Instagram and Messenger. And for ads with political content, we've created an archive that will hold ads with political content for seven years—including information about ad impressions and spend, as well as demographic data such as age, gender and location. People in Canada and Ireland have already been able to see all the ads that a Page is running on Facebook—and we've launched this globally.

- **Verification and labeling.** Every advertiser will now need to confirm their ID and location before being able to run any ads with political content in the US. All ads with political content will also clearly state who paid for them.

- **Updating targeting.** We want ads on Facebook to be safe and civil. We thoroughly review the targeting criteria advertisers can use to ensure they are consistent with our principles. As a result, we removed nearly one-third of the targeting segments used by the IRA. We continue to allow some criteria that people may find controversial. But we do see businesses marketing things like historical books, documentaries or television shows using them in legitimate ways.

- **Better technology.** Over the past year, we've gotten increasingly better at finding and disabling fake accounts. We now block millions of fake accounts each day as people try to create them—and before they've done any harm. This is thanks to improvements in machine learning and artificial intelligence, which can proactively identify suspicious behavior at a scale that was not possible before—without needing to look at the content itself.

- **Action to tackle fake news.** We are working hard to stop the spread of false news. We work with third-party fact-checking organizations to limit the spread of articles rated false. To reduce the spread of false news, we remove fake accounts and disrupt economic incentives for traffickers of misinformation. We also use various signals, including feedback from our community, to identify potential false news. In countries where we have partnerships with independent third-party fact-checkers, stories rated as false by those fact-checkers are shown lower in News Feed. If Pages or domains repeatedly create or share misinformation, we significantly reduce their distribution and remove their advertising rights. We also want to empower people to decide for themselves what to read, trust, and share. We promote news literacy and work to inform people with more context. For example, if third-party fact-checkers write articles about a news story, we show them immediately below the story in the Related Articles unit. We also notify people and Page Admins if they try to share a story, or have shared one in the past, that's been determined to be false. In addition to our own efforts, we're learning from academics, scaling our partnerships with third-party fact-checkers and talking to other

organizations about how we can work together.

A key focus is working to disrupt the economics of fake news. For example, preventing the creation of fake accounts that spread it, banning sites that engage in this behavior from using our ad products, and demoting articles found to be false by fact checkers in News Feed—causing it to lose 80% of its traffic. We now work with independent fact checkers in the US, France, Germany, Ireland, the Netherlands, Italy, Mexico, Colombia, India, Indonesia and the Philippines with plans to scale to more countries in the coming months.

- **Significant investments in security.** We're doubling the number of people working on safety and security from 10,000 last year to over 20,000 this year. We expect these investments to impact our profitability. But the safety of people using Facebook needs to come before profit.

- **Industry collaboration.** Recently, we joined 34 global tech and security companies in signing a TechAccord pact to help improve security for everyone.

- **Information sharing and reporting channels.** In the 2017 German elections, we worked closely with the authorities there, including the Federal Office for Information Security (BSI). This gave them a dedicated reporting channel for security issues related to the federal elections.

- **Tracking 40+ elections.** In recent months, we've started to deploy new tools and teams to proactively identify threats in the run-up to specific elections. We first tested this effort during the Alabama Senate election, and plan to continue these efforts for elections around the globe, including the US midterms. Last year we used public service announcements to help inform people about fake news in 21 separate countries, including in advance of French, Kenyan and German elections.

- **Action against the Russia-based IRA.** In April, we removed 70 Facebook and 65 Instagram accounts—as well as 138 Facebook Pages—controlled by the IRA primarily targeted either at people living in Russia or Russian-speakers around the world including from neighboring countries like Azerbaijan, Uzbekistan and Ukraine. The IRA has repeatedly used complex networks of inauthentic accounts to deceive and manipulate people in the US, Europe and Russia—and we don't want them on Facebook anywhere in the world.

343. What are you doing about Russian meddling? Have you investigated whether the Russian ads affected voter turnout in 2016? If not, why not? Did you collect the appropriate data to do so? Do you now collect the appropriate data? Are you setting up randomized experiments so that you can conduct such tests in future election cycles? (Note that this can be done even if you don't know which ads are Russian, or "fake news," or otherwise created to manipulate.)

For years, we had been aware of other types of activity that appeared to come from Russian sources—largely traditional security threats such as attacking people's accounts or using

social media platforms to spread stolen information. What we saw early in the 2016 campaign cycle followed this pattern. Our security team that focuses on threat intelligence—which investigates advanced security threats as part of our overall information security organization—was, from the outset, alert to the possibility of Russian activity. In several instances before November 8, 2016, this team detected and mitigated threats from actors with ties to Russia and reported them to US law enforcement officials. This included activity from a cluster of accounts we had assessed to belong to a group (APT28) that the US government has publicly linked to Russian military intelligence services. This activity, which was aimed at employees of major US political parties, fell into the normal categories of offensive cyber activities we monitor for. We warned the targets who were at highest risk, and were later in contact with law enforcement authorities about this activity.

Later in the summer we also started to see a new kind of behavior from APT28-related accounts—namely, the creation of fake personas that were then used to seed stolen information to journalists. These fake personas were organized under the banner of an organization that called itself DC Leaks. This activity violated our policies, and we removed the DC Leaks accounts.

Facebook learned from press accounts and statements by congressional leaders that Russian actors might have tried to interfere in the 2016 election by exploiting Facebook's ad tools. This is not something we had seen before, and so we started an investigation. We found that fake accounts associated with the IRA tried to influence the election.

This will never be a solved problem because we're up against determined, creative and well-funded adversaries. But we are making steady progress in preventing bad actors from using misinformation to undermine the democratic process, such as: increased ad transparency, advertiser verification and labeling, updating targeting criteria, better technological efforts to find and disable fake accounts, third-party fact checking to stop the spread of false news, doubling the number of people working on safety and security, greater industry collaboration, increased information sharing and reporting channels, proactive identification of election threats, and specific action against the Russia-based IRA.

We will continue to work with the government, and across the tech industry and civil society, to address this important national security matter so that we can do our part to prevent similar abuse from happening again.

344. How come when Zuckerberg helped the Obama campaign in 2012 to harvest Facebook data, the Democrats never complained?

We want our platform to be a place where people can have authentic conversations about elections and other political topics. We believe this kind of engagement promotes democracy, but we know that there are actors working to interfere with those conversations and undermine our elections. We are already taking steps to proactively prevent election interference and we are strengthening these protections going forward.

Engagement with campaigns: We want all candidates, groups, and voters to use our platform to engage in elections. We want it to be easy for people to find, follow, and contact

their elected representatives—and those running to represent them. That's why, for candidates across the political spectrum, Facebook offers the same levels of support in key moments to help campaigns understand how best to use the platform. Both the Obama and Romney campaigns had access to the same tools, and no campaign received any special treatment from Facebook. Likewise, we offered identical support to both the Trump and Clinton campaigns, and had teams assigned to both. Everyone had access to the same tools, which are the same tools that every campaign is offered, and is consistent with support provided to commercial clients in the normal course of business. Facebook representatives advise political advertisers on Facebook, as they would with other, non-political managed accounts. We have a compliance team that trains our sales representatives to comply with all federal election law requirements in this area.

While no one from Facebook was assigned full-time to the Trump campaign, Facebook employees did interact with Cambridge Analytica employees. While our investigation is ongoing, our review indicates that Facebook employees did not identify any issues involving the improper use of Facebook data in the course of their interactions with Cambridge Analytica during the 2016 US Presidential campaign.

Election Integrity: In the run-up to the 2016 elections, we were focused on the kinds of cybersecurity attacks typically used by nation states, for example phishing and malware attacks. And we were too slow to spot information operations interference. Since then, we've made important changes to prevent bad actors from using misinformation to undermine the democratic process. This will never be a solved problem because we're up against determined, creative and well-funded adversaries. But we are making steady progress. Here is a list of the 10 most important changes we have made:

- **Ads transparency.** Advertising should be transparent: users should be able to see all the ads an advertiser is currently running on Facebook, Instagram and Messenger. And for ads with political content, we've created an archive that will hold ads with political content for seven years—including information about ad impressions and spend, as well as demographic data such as age, gender and location. People in Canada and Ireland have already been able to see all the ads that a Page is running on Facebook—and we've launched this globally.

- **Verification and labeling.** Every advertiser will now need to confirm their ID and location before being able to run any ads with political content in the US. All ads with political content will also clearly state who paid for them.

- **Updating targeting.** We want ads on Facebook to be safe and civil. We thoroughly review the targeting criteria advertisers can use to ensure they are consistent with our principles. As a result, we removed nearly one-third of the targeting segments used by the IRA. We continue to allow some criteria that people may find controversial. But we do see businesses marketing things like historical books, documentaries or television shows using them in legitimate ways.

- **Better technology.** Over the past year, we've gotten increasingly better at finding and disabling fake accounts. We now block millions of fake accounts each day as people try to create them—and before they've done any harm. This is thanks to improvements in

machine learning and artificial intelligence, which can proactively identify suspicious behavior at a scale that was not possible before—without needing to look at the content itself.

- **Action to tackle fake news.** We are working hard to stop the spread of false news. We work with third-party fact-checking organizations to limit the spread of articles rated false. To reduce the spread of false news, we remove fake accounts and disrupt economic incentives for traffickers of misinformation. We also use various signals, including feedback from our community, to identify potential false news. In countries where we have partnerships with independent third-party fact-checkers, stories rated as false by those fact-checkers are shown lower in News Feed. If Pages or domains repeatedly create or share misinformation, we significantly reduce their distribution and remove their advertising rights. We also want to empower people to decide for themselves what to read, trust, and share. We promote news literacy and work to inform people with more context. For example, if third-party fact-checkers write articles about a news story, we show them immediately below the story in the Related Articles unit. We also notify people and Page Admins if they try to share a story, or have shared one in the past, that's been determined to be false. In addition to our own efforts, we're learning from academics, scaling our partnerships with third-party fact-checkers and talking to other organizations about how we can work together.

  A key focus is working to disrupt the economics of fake news. For example, preventing the creation of fake accounts that spread it, banning sites that engage in this behavior from using our ad products, and demoting articles found to be false by fact checkers in News Feed—causing it to lose 80% of its traffic. We now work with independent fact checkers in the US, France, Germany, Ireland, the Netherlands, Italy, Mexico, Colombia, India, Indonesia and the Philippines with plans to scale to more countries in the coming months.

- **Significant investments in security.** We're doubling the number of people working on safety and security from 10,000 last year to over 20,000 this year. We expect these investments to impact our profitability. But the safety of people using Facebook needs to come before profit.

- **Industry collaboration.** Recently, we joined 34 global tech and security companies in signing a TechAccord pact to help improve security for everyone.

- **Information sharing and reporting channels.** In the 2017 German elections, we worked closely with the authorities there, including the Federal Office for Information Security (BSI). This gave them a dedicated reporting channel for security issues related to the federal elections.

- **Tracking 40+ elections.** In recent months, we've started to deploy new tools and teams to proactively identify threats in the run-up to specific elections. We first tested this effort during the Alabama Senate election, and plan to continue these efforts for elections around the globe, including the US midterms. Last year we used public service

announcements to help inform people about fake news in 21 separate countries, including in advance of French, Kenyan and German elections.

- **Action against the Russia-based IRA.** In April, we removed 70 Facebook and 65 Instagram accounts—as well as 138 Facebook Pages—controlled by the IRA primarily targeted either at people living in Russia or Russian-speakers around the world including from neighboring countries like Azerbaijan, Uzbekistan and Ukraine. The IRA has repeatedly used complex networks of inauthentic accounts to deceive and manipulate people in the US, Europe and Russia—and we don't want them on Facebook anywhere in the world.

345. How can you stop users from posting "fake news"?

We want Facebook to be a place where people can discover more news, information, and perspectives, and we are working to build products that help to that. Through our News Feed algorithm, we also work hard to actively reduce the distribution of clickbait, sensationalism, and misinformation, on the one hand, and to boost news and information from sources that are trusted, informative, and local, on the other hand.
We are focusing on four different strategies to address misinformation:

- **Strengthening enforcement of our authenticity policies.** We are investing heavily in new technology and hiring thousands more people to tackle the problem of inauthenticity on the platform. Fake accounts are often associated with false news, so this is an area that will have a huge impact on curbing the spread of inaccurate information.

- **Finding industry solutions.** All of us—from tech companies and media companies to newsrooms and classrooms—must work together to find industry solutions to strengthen the online news ecosystem and our own digital literacy. That's why we're collaborating with others who operate in this space. Last January, we announced The Facebook Journalism Project, an initiative that seeks to establish stronger ties between Facebook and the news industry. The project is focused on developing news products, providing training and tools for journalists, and working with publishers and educators on how we can equip people with the knowledge they need to be informed readers in the digital age. Since launching the Journalism Project, we've met with more than 2,600 publishers around the world to understand how they use our products and how we can make improvements to better support their needs.

- **Disrupting economic incentives.** When it comes to fighting false news, we've found that a lot of it is financially motivated. So, one of the most effective approaches is removing the economic incentives for those who traffic in inaccurate information. We've done things like block ads from pages that repeatedly share false news and significantly limit the distribution of web pages that deliver low quality web experiences.

- **Building new products.** We believe it's important to amplify the good effects of social media and mitigate the bad—to contribute to the diversity of ideas, information, and view points, while strengthening our common understanding.

- We believe giving people more context can help them decide what to trust and what to share. The third-party fact-checking program we have developed uses reports from our community, along with other signals, to send stories to accredited third-party fact checking organizations. If the fact checking organizations identify a story as fake, we will suggest related articles in News Feed to show people different points of view, including information from fact checkers. Stories that have been disputed may also appear lower in News Feed. Our own data analytics show that a false rating from one of our fact checking partners reduces future impressions on Facebook by 80 percent.

- We're also testing Article Context as a way of giving people more information about the material they're reading on Facebook. Since we launched this test, some of the articles people see in News Feed will feature an "i" icon that allows them to access more information at the tap of a button. The information we surface is pulled from across the internet, and includes things like the publisher's Wikipedia entry, trending articles or related articles about the topic, and information about how the article is being shared on Facebook. In some cases, if that information is unavailable, we will let people know since that can also be helpful context.

346. What responsibility do you think a company like Facebook has in the proliferation of fake news?

We want Facebook to be a place where people can discover more news, information, and perspectives, and we are working to build products that help to that. Through our News Feed algorithm, we also work hard to actively reduce the distribution of clickbait, sensationalism, and misinformation, on the one hand, and to boost news and information from sources that are trusted, informative, and local, on the other hand.
We are focusing on four different strategies to address misinformation:

- **Strengthening enforcement of our authenticity policies.** We are investing heavily in new technology and hiring thousands more people to tackle the problem of inauthenticity on the platform. Fake accounts are often associated with false news, so this is an area that will have a huge impact on curbing the spread of inaccurate information.

- **Finding industry solutions.** All of us—from tech companies and media companies to newsrooms and classrooms—must work together to find industry solutions to strengthen the online news ecosystem and our own digital literacy. That's why we're collaborating with others who operate in this space. Last January, we announced The Facebook Journalism Project, an initiative that seeks to establish stronger ties between Facebook and the news industry. The project is focused on developing news products, providing training and tools for journalists, and working with publishers and educators on how we can equip people with the knowledge they need to be informed readers in the digital age. Since launching the Journalism Project, we've met with more than 2,600 publishers around the world to understand how they use our products and how we can make improvements to better support their needs.

- **Disrupting economic incentives.** When it comes to fighting false news, we've found that a lot of it is financially motivated. So, one of the most effective approaches is removing the economic incentives for those who traffic in inaccurate information. We've done things like block ads from pages that repeatedly share false news and significantly limit the distribution of web pages that deliver low quality web experiences.

- **Building new products.** We believe it's important to amplify the good effects of social media and mitigate the bad—to contribute to the diversity of ideas, information, and view points, while strengthening our common understanding.

    - We believe giving people more context can help them decide what to trust and what to share. The third-party fact-checking program we have developed uses reports from our community, along with other signals, to send stories to accredited third-party fact checking organizations. If the fact checking organizations identify a story as fake, we will suggest related articles in News Feed to show people different points of view, including information from fact checkers. Stories that have been disputed may also appear lower in News Feed. Our own data analytics show that a false rating from one of our fact checking partners reduces future impressions on Facebook by 80 percent.

    - We're also testing Article Context as a way of giving people more information about the material they're reading on Facebook. Since we launched this test, some of the articles people see in News Feed will feature an "i" icon that allows them to access more information at the tap of a button. The information we surface is pulled from across the internet, and includes things like the publisher's Wikipedia entry, trending articles or related articles about the topic, and information about how the article is being shared on Facebook. In some cases, if that information is unavailable, we will let people know since that can also be helpful context.

347. Should Facebook individual users expect that their political expressions or 'profile' will not be shared internally or externally (beyond their 'friends' settings)—as the "default" setup, meaning, not available to Advertisers unless explicitly authorized?

To build a secure product with extensive infrastructure that connects people wherever they live or whatever their income level, we need to make sure everyone can afford it. Advertising lets us keep Facebook free, which ensures it remains affordable for everyone. We also believe the ads you see across the Facebook family of apps and services should be useful and relevant to you. Users can't opt out of seeing ads altogether because selling ads is what keeps Facebook free, but they do have different options to control how their data can and can't be used to show them ads. They're all found in ad preferences, which allows users to turn off the use of all data collected from partners off Facebook to target ads. Users can also decide which of their profile fields they want used for ad targeting in the Information section under "About you." Users can remove themselves from interests under "Your interests" and categories under "Your categories." And, we do not sell people's information to anyone, and we never will.

Facebook is committed to transparency for all ads, including ads with political content. Facebook believes that people should be able to easily understand why they are seeing ads, who

paid for them, and what other ads those advertisers are running. As such, Facebook only allows authorized advertisers to run ads about elections or issues that are being debated across the country. In order to be authorized by Facebook, advertisers will need to confirm their identity and location. Furthermore, all political and issue ads will include a disclosure which reads: "Paid for by," and when users click on this disclosure they will be able to see details about the advertiser. Users will also be able to see an explanation of why they saw the particular ad. This is similar to the disclosure included on political TV advertisements. We just launched globally View Active Ads, a feature that will enable anyone to see all of the ads an advertiser is currently running by visiting the advertiser's Facebook Page.

348. Were there no early warnings of the Russian trolls?

For years, we had been aware of other types of activity that appeared to come from Russian sources—largely traditional security threats such as attacking people's accounts or using social media platforms to spread stolen information. What we saw early in the 2016 campaign cycle followed this pattern. Our security team that focuses on threat intelligence—which investigates advanced security threats as part of our overall information security organization—was, from the outset, alert to the possibility of Russian activity. In several instances before November 8, 2016, this team detected and mitigated threats from actors with ties to Russia and reported them to US law enforcement officials. This included activity from a cluster of accounts we had assessed to belong to a group (APT28) that the US government has publicly linked to Russian military intelligence services. This activity, which was aimed at employees of major US political parties, fell into the normal categories of offensive cyber activities we monitor for. We warned the targets who were at highest risk, and were later in contact with law enforcement authorities about this activity.

Later in the summer we also started to see a new kind of behavior from APT28-related accounts—namely, the creation of fake personas that were then used to seed stolen information to journalists. These fake personas were organized under the banner of an organization that called itself DC Leaks. This activity violated our policies, and we removed the DC Leaks accounts.

Facebook learned from press accounts and statements by congressional leaders that Russian actors might have tried to interfere in the 2016 election by exploiting Facebook's ad tools. This is not something we had seen before, and so we started an investigation. We found that fake accounts associated with the IRA tried to influence the election.

This will never be a solved problem because we're up against determined, creative and well-funded adversaries. But we are making steady progress in preventing bad actors from using misinformation to undermine the democratic process, such as: increased ad transparency, advertiser verification and labeling, updating targeting criteria, better technological efforts to find and disable fake accounts, third-party fact checking to stop the spread of false news, doubling the number of people working on safety and security, greater industry collaboration, increased information sharing and reporting channels, proactive identification of election threats, and specific action against the Russia-based IRA.

We will continue to work with the government, and across the tech industry and civil society, to address this important national security matter so that we can do our part to prevent similar abuse from happening again.

349. What is Facebook doing to fight fake news?

We want Facebook to be a place where people can discover more news, information, and perspectives, and we are working to build products that help to that. Through our News Feed algorithm, we also work hard to actively reduce the distribution of clickbait, sensationalism, and misinformation, on the one hand, and to boost news and information from sources that are trusted, informative, and local, on the other hand.

We are focusing on four different strategies to address misinformation:

- **Strengthening enforcement of our authenticity policies.** We are investing heavily in new technology and hiring thousands more people to tackle the problem of inauthenticity on the platform. Fake accounts are often associated with false news, so this is an area that will have a huge impact on curbing the spread of inaccurate information.

- **Finding industry solutions.** All of us—from tech companies and media companies to newsrooms and classrooms—must work together to find industry solutions to strengthen the online news ecosystem and our own digital literacy. That's why we're collaborating with others who operate in this space. Last January, we announced The Facebook Journalism Project, an initiative that seeks to establish stronger ties between Facebook and the news industry. The project is focused on developing news products, providing training and tools for journalists, and working with publishers and educators on how we can equip people with the knowledge they need to be informed readers in the digital age. Since launching the Journalism Project, we've met with more than 2,600 publishers around the world to understand how they use our products and how we can make improvements to better support their needs.

- **Disrupting economic incentives.** When it comes to fighting false news, we've found that a lot of it is financially motivated. So, one of the most effective approaches is removing the economic incentives for those who traffic in inaccurate information. We've done things like block ads from pages that repeatedly share false news and significantly limit the distribution of web pages that deliver low quality web experiences.

- **Building new products.** We believe it's important to amplify the good effects of social media and mitigate the bad—to contribute to the diversity of ideas, information, and view points, while strengthening our common understanding.

    - We believe giving people more context can help them decide what to trust and what to share. The third-party fact-checking program we have developed uses reports from our community, along with other signals, to send stories to accredited third-party fact checking organizations. If the fact checking organizations identify a story as fake, we will suggest related articles in News Feed to show people different points of view, including information from fact checkers. Stories that have been disputed may also appear lower in News Feed.

Our own data analytics show that a false rating from one of our fact checking partners reduces future impressions on Facebook by 80 percent.

- We're also testing Article Context as a way of giving people more information about the material they're reading on Facebook. Since we launched this test, some of the articles people see in News Feed will feature an "i" icon that allows them to access more information at the tap of a button. The information we surface is pulled from across the internet, and includes things like the publisher's Wikipedia entry, trending articles or related articles about the topic, and information about how the article is being shared on Facebook. In some cases, if that information is unavailable, we will let people know since that can also be helpful context.

350. What about the 2012 election when people were applauding Obama for data mining?

We want our platform to be a place where people can have authentic conversations about elections and other political topics. We believe this kind of engagement promotes democracy, but we know that there are actors working to interfere with those conversations and undermine our elections. We are already taking steps to proactively prevent election interference and we are strengthening these protections going forward.

Engagement with campaigns: We want all candidates, groups, and voters to use our platform to engage in elections. We want it to be easy for people to find, follow, and contact their elected representatives—and those running to represent them. That's why, for candidates across the political spectrum, Facebook offers the same levels of support in key moments to help campaigns understand how best to use the platform. Both the Obama and Romney campaigns had access to the same tools, and no campaign received any special treatment from Facebook. Likewise, we offered identical support to both the Trump and Clinton campaigns, and had teams assigned to both. Everyone had access to the same tools, which are the same tools that every campaign is offered, and is consistent with support provided to commercial clients in the normal course of business. Facebook representatives advise political advertisers on Facebook, as they would with other, non-political managed accounts. We have a compliance team that trains our sales representatives to comply with all federal election law requirements in this area.

While no one from Facebook was assigned full-time to the Trump campaign, Facebook employees did interact with Cambridge Analytica employees. While our investigation is ongoing, our review indicates that Facebook employees did not identify any issues involving the improper use of Facebook data in the course of their interactions with Cambridge Analytica during the 2016 US Presidential campaign.

Election Integrity: In the run-up to the 2016 elections, we were focused on the kinds of cybersecurity attacks typically used by nation states, for example phishing and malware attacks. And we were too slow to spot information operations interference. Since then, we've made important changes to prevent bad actors from using misinformation to undermine the democratic process. This will never be a solved problem because we're up against determined, creative and well-funded adversaries. But we are making steady progress. Here is a list of the 10 most important changes we have made:

- **Ads transparency.** Advertising should be transparent: users should be able to see all the ads an advertiser is currently running on Facebook, Instagram and Messenger. And for ads with political content, we've created an archive that will hold ads with political content for seven years—including information about ad impressions and spend, as well as demographic data such as age, gender and location. People in Canada and Ireland have already been able to see all the ads that a Page is running on Facebook—and we've launched this globally.

- **Verification and labeling.** Every advertiser will now need to confirm their ID and location before being able to run any ads with political content in the US. All ads with political content will also clearly state who paid for them.

- **Updating targeting.** We want ads on Facebook to be safe and civil. We thoroughly review the targeting criteria advertisers can use to ensure they are consistent with our principles. As a result, we removed nearly one-third of the targeting segments used by the IRA. We continue to allow some criteria that people may find controversial. But we do see businesses marketing things like historical books, documentaries or television shows using them in legitimate ways.

- **Better technology.** Over the past year, we've gotten increasingly better at finding and disabling fake accounts. We now block millions of fake accounts each day as people try to create them—and before they've done any harm. This is thanks to improvements in machine learning and artificial intelligence, which can proactively identify suspicious behavior at a scale that was not possible before—without needing to look at the content itself.

- **Action to tackle fake news.** We are working hard to stop the spread of false news. We work with third-party fact-checking organizations to limit the spread of articles rated false. To reduce the spread of false news, we remove fake accounts and disrupt economic incentives for traffickers of misinformation. We also use various signals, including feedback from our community, to identify potential false news. In countries where we have partnerships with independent third-party fact-checkers, stories rated as false by those fact-checkers are shown lower in News Feed. If Pages or domains repeatedly create or share misinformation, we significantly reduce their distribution and remove their advertising rights. We also want to empower people to decide for themselves what to read, trust, and share. We promote news literacy and work to inform people with more context. For example, if third-party fact-checkers write articles about a news story, we show them immediately below the story in the Related Articles unit. We also notify people and Page Admins if they try to share a story, or have shared one in the past, that's been determined to be false. In addition to our own efforts, we're learning from academics, scaling our partnerships with third-party fact-checkers and talking to other organizations about how we can work together.

  A key focus is working to disrupt the economics of fake news. For example, preventing the creation of fake accounts that spread it, banning sites that engage in this behavior from using our ad products, and demoting articles found to be false by fact checkers in

News Feed—causing it to lose 80% of its traffic. We now work with independent fact checkers in the US, France, Germany, Ireland, the Netherlands, Italy, Mexico, Colombia, India, Indonesia and the Philippines with plans to scale to more countries in the coming months.

- **Significant investments in security.** We're doubling the number of people working on safety and security from 10,000 last year to over 20,000 this year. We expect these investments to impact our profitability. But the safety of people using Facebook needs to come before profit.

- **Industry collaboration.** Recently, we joined 34 global tech and security companies in signing a TechAccord pact to help improve security for everyone.

- **Information sharing and reporting channels.** In the 2017 German elections, we worked closely with the authorities there, including the Federal Office for Information Security (BSI). This gave them a dedicated reporting channel for security issues related to the federal elections.

- **Tracking 40+ elections.** In recent months, we've started to deploy new tools and teams to proactively identify threats in the run-up to specific elections. We first tested this effort during the Alabama Senate election, and plan to continue these efforts for elections around the globe, including the US midterms. Last year we used public service announcements to help inform people about fake news in 21 separate countries, including in advance of French, Kenyan and German elections.

- **Action against the Russia-based IRA.** In April, we removed 70 Facebook and 65 Instagram accounts—as well as 138 Facebook Pages—controlled by the IRA primarily targeted either at people living in Russia or Russian-speakers around the world including from neighboring countries like Azerbaijan, Uzbekistan and Ukraine. The IRA has repeatedly used complex networks of inauthentic accounts to deceive and manipulate people in the US, Europe and Russia—and we don't want them on Facebook anywhere in the world.

351. How do you plan to protect the public from the insurgence of fake news on your platform, which continues to threaten our democracy, particularly as it relates to the 2018 midterms?

We want Facebook to be a place where people can discover more news, information, and perspectives, and we are working to build products that help to that. Through our News Feed algorithm, we also work hard to actively reduce the distribution of clickbait, sensationalism, and misinformation, on the one hand, and to boost news and information from sources that are trusted, informative, and local, on the other hand.

We are focusing on four different strategies to address misinformation:

- **Strengthening enforcement of our authenticity policies.** We are investing heavily in new technology and hiring thousands more people to tackle the problem of inauthenticity

on the platform. Fake accounts are often associated with false news, so this is an area that will have a huge impact on curbing the spread of inaccurate information.

- **Finding industry solutions.** All of us—from tech companies and media companies to newsrooms and classrooms—must work together to find industry solutions to strengthen the online news ecosystem and our own digital literacy. That's why we're collaborating with others who operate in this space. Last January, we announced The Facebook Journalism Project, an initiative that seeks to establish stronger ties between Facebook and the news industry. The project is focused on developing news products, providing training and tools for journalists, and working with publishers and educators on how we can equip people with the knowledge they need to be informed readers in the digital age. Since launching the Journalism Project, we've met with more than 2,600 publishers around the world to understand how they use our products and how we can make improvements to better support their needs.

- **Disrupting economic incentives.** When it comes to fighting false news, we've found that a lot of it is financially motivated. So, one of the most effective approaches is removing the economic incentives for those who traffic in inaccurate information. We've done things like block ads from pages that repeatedly share false news and significantly limit the distribution of web pages that deliver low quality web experiences.

- **Building new products.** We believe it's important to amplify the good effects of social media and mitigate the bad—to contribute to the diversity of ideas, information, and view points, while strengthening our common understanding.

    - We believe giving people more context can help them decide what to trust and what to share. The third-party fact-checking program we have developed uses reports from our community, along with other signals, to send stories to accredited third-party fact checking organizations. If the fact checking organizations identify a story as fake, we will suggest related articles in News Feed to show people different points of view, including information from fact checkers. Stories that have been disputed may also appear lower in News Feed. Our own data analytics show that a false rating from one of our fact checking partners reduces future impressions on Facebook by 80 percent.

    - We're also testing Article Context as a way of giving people more information about the material they're reading on Facebook. Since we launched this test, some of the articles people see in News Feed will feature an "i" icon that allows them to access more information at the tap of a button. The information we surface is pulled from across the internet, and includes things like the publisher's Wikipedia entry, trending articles or related articles about the topic, and information about how the article is being shared on Facebook. In some cases, if that information is unavailable, we will let people know since that can also be helpful context.

352. What can Facebook do to block Russian interference in our elections?

For years, we had been aware of other types of activity that appeared to come from Russian sources—largely traditional security threats such as attacking people's accounts or using social media platforms to spread stolen information. What we saw early in the 2016 campaign cycle followed this pattern. Our security team that focuses on threat intelligence—which investigates advanced security threats as part of our overall information security organization—was, from the outset, alert to the possibility of Russian activity. In several instances before November 8, 2016, this team detected and mitigated threats from actors with ties to Russia and reported them to US law enforcement officials. This included activity from a cluster of accounts we had assessed to belong to a group (APT28) that the US government has publicly linked to Russian military intelligence services. This activity, which was aimed at employees of major US political parties, fell into the normal categories of offensive cyber activities we monitor for. We warned the targets who were at highest risk, and were later in contact with law enforcement authorities about this activity.

Later in the summer we also started to see a new kind of behavior from APT28-related accounts—namely, the creation of fake personas that were then used to seed stolen information to journalists. These fake personas were organized under the banner of an organization that called itself DC Leaks. This activity violated our policies, and we removed the DC Leaks accounts.

Facebook learned from press accounts and statements by congressional leaders that Russian actors might have tried to interfere in the 2016 election by exploiting Facebook's ad tools. This is not something we had seen before, and so we started an investigation. We found that fake accounts associated with the IRA tried to influence the election.

This will never be a solved problem because we're up against determined, creative and well-funded adversaries. But we are making steady progress in preventing bad actors from using misinformation to undermine the democratic process, such as: increased ad transparency, advertiser verification and labeling, updating targeting criteria, better technological efforts to find and disable fake accounts, third-party fact checking to stop the spread of false news, doubling the number of people working on safety and security, greater industry collaboration, increased information sharing and reporting channels, proactive identification of election threats, and specific action against the Russia-based IRA.

We will continue to work with the government, and across the tech industry and civil society, to address this important national security matter so that we can do our part to prevent similar abuse from happening again.

353. Please list all of the companies that are paying to disseminate false information on your platform?

We want Facebook to be a place where people can discover more news, information, and perspectives, and we are working to build products that help to that. Through our News Feed algorithm, we also work hard to actively reduce the distribution of clickbait, sensationalism, and misinformation, on the one hand, and to boost news and information from sources that are trusted, informative, and local, on the other hand.
We are focusing on four different strategies to address misinformation:

- **Strengthening enforcement of our authenticity policies.** We are investing heavily in new technology and hiring thousands more people to tackle the problem of inauthenticity on the platform. Fake accounts are often associated with false news, so this is an area that will have a huge impact on curbing the spread of inaccurate information.

- **Finding industry solutions.** All of us—from tech companies and media companies to newsrooms and classrooms—must work together to find industry solutions to strengthen the online news ecosystem and our own digital literacy. That's why we're collaborating with others who operate in this space. Last January, we announced The Facebook Journalism Project, an initiative that seeks to establish stronger ties between Facebook and the news industry. The project is focused on developing news products, providing training and tools for journalists, and working with publishers and educators on how we can equip people with the knowledge they need to be informed readers in the digital age. Since launching the Journalism Project, we've met with more than 2,600 publishers around the world to understand how they use our products and how we can make improvements to better support their needs.

- **Disrupting economic incentives.** When it comes to fighting false news, we've found that a lot of it is financially motivated. So, one of the most effective approaches is removing the economic incentives for those who traffic in inaccurate information. We've done things like block ads from pages that repeatedly share false news and significantly limit the distribution of web pages that deliver low quality web experiences.

- **Building new products.** We believe it's important to amplify the good effects of social media and mitigate the bad—to contribute to the diversity of ideas, information, and view points, while strengthening our common understanding.

    - We believe giving people more context can help them decide what to trust and what to share. The third-party fact-checking program we have developed uses reports from our community, along with other signals, to send stories to accredited third-party fact checking organizations. If the fact checking organizations identify a story as fake, we will suggest related articles in News Feed to show people different points of view, including information from fact checkers. Stories that have been disputed may also appear lower in News Feed. Our own data analytics show that a false rating from one of our fact checking partners reduces future impressions on Facebook by 80 percent.

    - We're also testing Article Context as a way of giving people more information about the material they're reading on Facebook. Since we launched this test, some of the articles people see in News Feed will feature an "i" icon that allows them to access more information at the tap of a button. The information we surface is pulled from across the internet, and includes things like the publisher's Wikipedia entry, trending articles or related articles about the topic, and information about how the article is being shared on Facebook. In some cases, if that information is unavailable, we will let people know since that can also be helpful context.

354. Please ask him if he believes meddling in US election process is here to stay and something we need to realize is real.

We want our platform to be a place where people can have authentic conversations about elections and other political topics. We believe this kind of engagement promotes democracy, but we know that there are actors working to interfere with those conversations and undermine our elections. We are already taking steps to proactively prevent election interference and we are strengthening these protections going forward.

Engagement with campaigns: We want all candidates, groups, and voters to use our platform to engage in elections. We want it to be easy for people to find, follow, and contact their elected representatives—and those running to represent them. That's why, for candidates across the political spectrum, Facebook offers the same levels of support in key moments to help campaigns understand how best to use the platform. Both the Obama and Romney campaigns had access to the same tools, and no campaign received any special treatment from Facebook. Likewise, we offered identical support to both the Trump and Clinton campaigns, and had teams assigned to both. Everyone had access to the same tools, which are the same tools that every campaign is offered, and is consistent with support provided to commercial clients in the normal course of business. Facebook representatives advise political advertisers on Facebook, as they would with other, non-political managed accounts. We have a compliance team that trains our sales representatives to comply with all federal election law requirements in this area.

While no one from Facebook was assigned full-time to the Trump campaign, Facebook employees did interact with Cambridge Analytica employees. While our investigation is ongoing, our review indicates that Facebook employees did not identify any issues involving the improper use of Facebook data in the course of their interactions with Cambridge Analytica during the 2016 US Presidential campaign.

Election Integrity: In the run-up to the 2016 elections, we were focused on the kinds of cybersecurity attacks typically used by nation states, for example phishing and malware attacks. And we were too slow to spot information operations interference. Since then, we've made important changes to prevent bad actors from using misinformation to undermine the democratic process. This will never be a solved problem because we're up against determined, creative and well-funded adversaries. But we are making steady progress. Here is a list of the 10 most important changes we have made:

- **Ads transparency.** Advertising should be transparent: users should be able to see all the ads an advertiser is currently running on Facebook, Instagram and Messenger. And for ads with political content, we've created an archive that will hold ads with political content for seven years—including information about ad impressions and spend, as well as demographic data such as age, gender and location. People in Canada and Ireland have already been able to see all the ads that a Page is running on Facebook—and we've launched this globally.

- **Verification and labeling.** Every advertiser will now need to confirm their ID and location before being able to run any ads with political content in the US. All ads with political content will also clearly state who paid for them.

- **Updating targeting.** We want ads on Facebook to be safe and civil. We thoroughly review the targeting criteria advertisers can use to ensure they are consistent with our principles. As a result, we removed nearly one-third of the targeting segments used by the IRA. We continue to allow some criteria that people may find controversial. But we do see businesses marketing things like historical books, documentaries or television shows using them in legitimate ways.

- **Better technology.** Over the past year, we've gotten increasingly better at finding and disabling fake accounts. We now block millions of fake accounts each day as people try to create them—and before they've done any harm. This is thanks to improvements in machine learning and artificial intelligence, which can proactively identify suspicious behavior at a scale that was not possible before—without needing to look at the content itself.

- **Action to tackle fake news.** We are working hard to stop the spread of false news. We work with third-party fact-checking organizations to limit the spread of articles rated false. To reduce the spread of false news, we remove fake accounts and disrupt economic incentives for traffickers of misinformation. We also use various signals, including feedback from our community, to identify potential false news. In countries where we have partnerships with independent third-party fact-checkers, stories rated as false by those fact-checkers are shown lower in News Feed. If Pages or domains repeatedly create or share misinformation, we significantly reduce their distribution and remove their advertising rights. We also want to empower people to decide for themselves what to read, trust, and share. We promote news literacy and work to inform people with more context. For example, if third-party fact-checkers write articles about a news story, we show them immediately below the story in the Related Articles unit. We also notify people and Page Admins if they try to share a story, or have shared one in the past, that's been determined to be false. In addition to our own efforts, we're learning from academics, scaling our partnerships with third-party fact-checkers and talking to other organizations about how we can work together.

  A key focus is working to disrupt the economics of fake news. For example, preventing the creation of fake accounts that spread it, banning sites that engage in this behavior from using our ad products, and demoting articles found to be false by fact checkers in News Feed—causing it to lose 80% of its traffic. We now work with independent fact checkers in the US, France, Germany, Ireland, the Netherlands, Italy, Mexico, Colombia, India, Indonesia and the Philippines with plans to scale to more countries in the coming months.

- **Significant investments in security.** We're doubling the number of people working on safety and security from 10,000 last year to over 20,000 this year. We expect these investments to impact our profitability. But the safety of people using Facebook needs to come before profit.

- **Industry collaboration.** Recently, we joined 34 global tech and security companies in signing a TechAccord pact to help improve security for everyone.

- **Information sharing and reporting channels.** In the 2017 German elections, we worked closely with the authorities there, including the Federal Office for Information Security (BSI). This gave them a dedicated reporting channel for security issues related to the federal elections.

- **Tracking 40+ elections.** In recent months, we've started to deploy new tools and teams to proactively identify threats in the run-up to specific elections. We first tested this effort during the Alabama Senate election, and plan to continue these efforts for elections around the globe, including the US midterms. Last year we used public service announcements to help inform people about fake news in 21 separate countries, including in advance of French, Kenyan and German elections.

- **Action against the Russia-based IRA.** In April, we removed 70 Facebook and 65 Instagram accounts—as well as 138 Facebook Pages—controlled by the IRA primarily targeted either at people living in Russia or Russian-speakers around the world including from neighboring countries like Azerbaijan, Uzbekistan and Ukraine. The IRA has repeatedly used complex networks of inauthentic accounts to deceive and manipulate people in the US, Europe and Russia—and we don't want them on Facebook anywhere in the world.

355. Why is Facebook being less than totally open to investigation of misuse?

Facebook's policies regarding third-party usage of its platform technologies have prohibited—and continue to prohibit third-party app developers from selling or licensing user data obtained from Facebook and from sharing any user data obtained from Facebook with any ad network, data broker or other advertising or monetization-related service.

We use a variety of tools to enforce Facebook policies against violating parties, including developers. We review tens of thousands of apps per year and regularly disapprove noncompliant apps as part of our proactive review process. We also use tools like cease and desist letters, account suspensions, letter agreements, and civil litigation. For example, since 2006, Facebook has sent over 1,150 cease-and-desist letters to over 1,600 targets. In 2017, we took action against about 370,000 apps, ranging from imposing certain restrictions to removal of the app from the platform. Moreover, we have required parties who have procured our data without authorization to delete that data. We have invested significant resources in these efforts.

Recently, we announced a number of additional steps we're taking to address concerns raised by Kogan's app.

- **Review our platform.** We will investigate all apps that had access to large amounts of data before the platform changes we announced in 2014, and we will audit any app where we identify suspicious activity. If we identify misuses of data, we'll take immediate action, including banning the app from our platform and pursuing legal action if appropriate.

- **Tell people about data misuse.** We will tell people about apps that have misused their data. This includes building a way for people to know if their data might have been accessed via the app. Moving forward, if we remove an app, we will tell people.

- **Turn off access for unused apps.** If someone has not used an app within the last three months, we will turn off the app's access to their data.

- **Restrict Facebook Login data.** We are changing Login, so that the only data that an app can request without app review will include name, profile photo, and email address. Requesting any other data will require approval from Facebook. We will also no longer allow apps to ask for access to information like religious or political views, relationship status and details, custom friends lists, education and work history, fitness activity, book reading and music listening activity, news reading, video watch activity, and games activity. We will encourage people to manage the apps they use. We already show people what apps their accounts are connected to and allow them to control what data they've permitted those apps to use. But we're making it easier for people to see what apps they use and the information they have shared with those apps.

- **Reward people who find vulnerabilities.** We launched the Data Abuse Bounty program so that people can report to us any misuses of data by app developers.

- **Update our policies.** We have updated our terms and Data Policy to explain how we use data and how data is shared with app developers.

356. Have any other third parties abused personal data to this extent, through Facebook, in the past?

Facebook's policies regarding third-party usage of its platform technologies have prohibited—and continue to prohibit—third-party app developers from selling or licensing user data obtained from Facebook and from sharing any user data obtained from Facebook with any ad network, data broker or other advertising or monetization-related service.

We use a variety of tools to enforce Facebook policies against violating parties, including developers. We review tens of thousands of apps per year and regularly disapprove noncompliant apps as part of our proactive review process. We also use tools like cease and desist letters, account suspensions, letter agreements, and civil litigation. For example, since 2006, Facebook has sent over 1,150 cease-and-desist letters to over 1,600 targets. In 2017, we took action against about 370,000 apps, ranging from imposing certain restrictions to removal of the app from the platform. Moreover, we have required parties who have procured our data without authorization to delete that data. We have invested significant resources in these efforts.

Recently, we announced a number of additional steps we're taking to address concerns raised by Kogan's app.

- **Review our platform.** We will investigate all apps that had access to large amounts of data before the platform changes we announced in 2014, and we will audit any app where we identify suspicious activity. If we identify misuses of data, we'll take immediate

action, including banning the app from our platform and pursuing legal action if appropriate.

- **Tell people about data misuse.** We will tell people about apps that have misused their data. This includes building a way for people to know if their data might have been accessed via the app. Moving forward, if we remove an app, we will tell people.

- **Turn off access for unused apps.** If someone has not used an app within the last three months, we will turn off the app's access to their data.

- **Restrict Facebook Login data.** We are changing Login, so that the only data that an app can request without app review will include name, profile photo, and email address. Requesting any other data will require approval from Facebook. We will also no longer allow apps to ask for access to information like religious or political views, relationship status and details, custom friends lists, education and work history, fitness activity, book reading and music listening activity, news reading, video watch activity, and games activity. We will encourage people to manage the apps they use. We already show people what apps their accounts are connected to and allow them to control what data they've permitted those apps to use. But we're making it easier for people to see what apps they use and the information they have shared with those apps.

- **Reward people who find vulnerabilities.** We launched the Data Abuse Bounty program so that people can report to us any misuses of data by app developers.

- **Update our policies.** We have updated our terms and Data Policy to explain how we use data and how data is shared with app developers.

357. Why doesn't he admit that making money has been and is his major goal and drives his business?

We believe everyone deserves good privacy controls. A user owns the information they share on Facebook. This means they decide what they share and who they share it with on Facebook, and they can change their mind. We require websites and apps who use our tools to tell users they're collecting and sharing their information with us, and to get users' permission to do so.

Everyone has the right to expect strong protections for their information. We also need to do our part to help keep our community safe, in a way that's consistent with people's privacy expectations. We've recently announced several steps to give people more control over their privacy, including a new Privacy Shortcuts tool that we're rolling out now to give people information about how to control their information, including choosing who can see what they post and adding protections like two-factor authentication to their account. People can learn more about how to protect their privacy in our updated Data Policy and in our Privacy Basics feature (https://www.facebook.com/about/basics).

We are in the process of investigating every app that had access to a large amount of information before we changed our Platform in 2014. The investigation process is in full swing. We have large teams of internal and external experts working hard to investigate these apps as

quickly as possible. As of early June 2018, thousands of apps have been investigated and around 200 apps have been suspended—pending a thorough investigation into whether they did in fact misuse any data. Where we find evidence that these or other apps did misuse data, we will ban them and let people know.

Facebook is generally not opposed to regulation but wants to ensure it is the right regulation. The issues facing the industry are complex, multi-faceted, and affect an important part of peoples' lives. As such, Facebook is absolutely committed to working with regulators, like Congress, to craft the right regulations. Facebook would be happy to review any proposed legislation and provide comments.

358. Facebook's business model is based on monetizing user's information. Why should we trust you?

We believe everyone deserves good privacy controls. A user owns the information they share on Facebook. This means they decide what they share and who they share it with on Facebook, and they can change their mind. We require websites and apps who use our tools to tell users they're collecting and sharing their information with us, and to get users' permission to do so.

Everyone has the right to expect strong protections for their information. We also need to do our part to help keep our community safe, in a way that's consistent with people's privacy expectations. We've recently announced several steps to give people more control over their privacy, including a new Privacy Shortcuts tool that we're rolling out now to give people information about how to control their information, including choosing who can see what they post and adding protections like two-factor authentication to their account. People can learn more about how to protect their privacy in our updated Data Policy and in our Privacy Basics feature (https://www.facebook.com/about/basics).

We are in the process of investigating every app that had access to a large amount of information before we changed our Platform in 2014. The investigation process is in full swing. We have large teams of internal and external experts working hard to investigate these apps as quickly as possible. As of early June 2018, thousands of apps have been investigated and around 200 apps have been suspended—pending a thorough investigation into whether they did in fact misuse any data. Where we find evidence that these or other apps did misuse data, we will ban them and let people know.

Facebook is generally not opposed to regulation but wants to ensure it is the right regulation. The issues facing the industry are complex, multi-faceted, and affect an important part of peoples' lives. As such, Facebook is absolutely committed to working with regulators, like Congress, to craft the right regulations. Facebook would be happy to review any proposed legislation and provide comments.

359. Given that your business model is based on selling personal data, how and why would you protect user data?

We believe everyone deserves good privacy controls. A user owns the information they share on Facebook. This means they decide what they share and who they share it with on

Facebook, and they can change their mind. We require websites and apps who use our tools to tell users they're collecting and sharing their information with us, and to get users' permission to do so.

Everyone has the right to expect strong protections for their information. We also need to do our part to help keep our community safe, in a way that's consistent with people's privacy expectations. We've recently announced several steps to give people more control over their privacy, including a new Privacy Shortcuts tool that we're rolling out now to give people information about how to control their information, including choosing who can see what they post and adding protections like two-factor authentication to their account. People can learn more about how to protect their privacy in our updated Data Policy and in our Privacy Basics feature (https://www.facebook.com/about/basics).

We are in the process of investigating every app that had access to a large amount of information before we changed our Platform in 2014. The investigation process is in full swing. We have large teams of internal and external experts working hard to investigate these apps as quickly as possible. As of early June 2018, thousands of apps have been investigated and around 200 apps have been suspended—pending a thorough investigation into whether they did in fact misuse any data. Where we find evidence that these or other apps did misuse data, we will ban them and let people know.

Facebook is generally not opposed to regulation but wants to ensure it is the right regulation. The issues facing the industry are complex, multi-faceted, and affect an important part of peoples' lives. As such, Facebook is absolutely committed to working with regulators, like Congress, to craft the right regulations. Facebook would be happy to review any proposed legislation and provide comments.

360. Will Facebook, at minimum, implement (not just make available) European Union's GDPR's rules everywhere with only a few exceptions?

As a part of our overall approach to privacy, we are providing the same tools for access, rectification, erasure, data portability and others to people in the US (and globally) that we provide in the European Union under the GDPR. The controls and settings that Facebook is enabling as part of GDPR include settings for controlling our use of face recognition on Facebook and for controlling our ability to use data we collect off Facebook Company Products to target ads. We recently began providing direct notice of these controls and our updated terms to people around the world (including in the US), allowing people to choose whether or not to enable or disable these settings or to consent to our updated terms. Many of these tools (like our Download Your Information tool, ad preferences tool, and Activity Log) have been available globally for many years.

However, the GDPR creates some specific requirements that do not apply in the rest of the world, for example the requirement to provide contact information for the EU Data Protection Officer or to specify legal bases for processing data. We are also looking to be more responsive to regional norms and legal frameworks going forward, and want to have the flexibility to work with local regulators, which is possible with this new model. At the same time, we are changing the provisions in our Facebook, Inc. terms in our user agreements outside

the United States to allow people in other countries to file lawsuits against Facebook in their home country, rather than in courts in the US. This transition was part of a continued effort to be locally responsive in countries where people use our services.

361. Why doesn't FB require all users to pass a ¿robot¿ check? Eliminate bots.

We want Facebook to be a place where people can discover more news, information, and perspectives, and we are working to build products that help to that. Through our News Feed algorithm, we also work hard to actively reduce the distribution of clickbait, sensationalism, and misinformation, on the one hand, and to boost news and information from sources that are trusted, informative, and local, on the other hand.

We are focusing on four different strategies to address misinformation:

- **Strengthening enforcement of our authenticity policies.** We are investing heavily in new technology and hiring thousands more people to tackle the problem of inauthenticity on the platform. Fake accounts are often associated with false news, so this is an area that will have a huge impact on curbing the spread of inaccurate information.

- **Finding industry solutions.** All of us—from tech companies and media companies to newsrooms and classrooms—must work together to find industry solutions to strengthen the online news ecosystem and our own digital literacy. That's why we're collaborating with others who operate in this space. Last January, we announced The Facebook Journalism Project, an initiative that seeks to establish stronger ties between Facebook and the news industry. The project is focused on developing news products, providing training and tools for journalists, and working with publishers and educators on how we can equip people with the knowledge they need to be informed readers in the digital age. Since launching the Journalism Project, we've met with more than 2,600 publishers around the world to understand how they use our products and how we can make improvements to better support their needs.

- **Disrupting economic incentives.** When it comes to fighting false news, we've found that a lot of it is financially motivated. So, one of the most effective approaches is removing the economic incentives for those who traffic in inaccurate information. We've done things like block ads from pages that repeatedly share false news and significantly limit the distribution of web pages that deliver low quality web experiences.

- **Building new products.** We believe it's important to amplify the good effects of social media and mitigate the bad—to contribute to the diversity of ideas, information, and view points, while strengthening our common understanding.

    - We believe giving people more context can help them decide what to trust and what to share. The third-party fact-checking program we have developed uses reports from our community, along with other signals, to send stories to accredited third-party fact checking organizations. If the fact checking organizations identify a story as fake, we will suggest related articles in News Feed to show people different points of view, including information from fact checkers. Stories that have been disputed may also appear lower in News Feed.

Our own data analytics show that a false rating from one of our fact checking partners reduces future impressions on Facebook by 80 percent.

- We're also testing Article Context as a way of giving people more information about the material they're reading on Facebook. Since we launched this test, some of the articles people see in News Feed will feature an "i" icon that allows them to access more information at the tap of a button. The information we surface is pulled from across the internet, and includes things like the publisher's Wikipedia entry, trending articles or related articles about the topic, and information about how the article is being shared on Facebook. In some cases, if that information is unavailable, we will let people know since that can also be helpful context.

362. Describe how your business philosophy distinguishes the harm to individuals from the harm to society

We recognize that we have made mistakes, and we are committed to learning from this experience to secure our platform further and make our community safer for everyone going forward. As our CEO Mark Zuckerberg has said, when you are building something unprecedented like Facebook, there are going to be mistakes. What people should hold us accountable for is learning from the mistakes and continually doing better—and, at the end of the day, making sure that we're building things that people like and that make their lives better.

Particularly in the past few months, we've realized that we need to take a broader view of our responsibility to our community. Part of that effort is continuing our ongoing efforts to identify ways that we can improve our privacy practices. We've heard loud and clear that privacy settings and other important tools are too hard to find and that we must do more to keep people informed. So, we're taking additional steps to put people more in control of their privacy. For instance, we redesigned our entire settings menu on mobile devices from top to bottom to make things easier to find. We also created a new Privacy Shortcuts in a menu where users can control their data in just a few taps, with clearer explanations of how our controls work. The experience is now clearer, more visual, and easy-to-find. Furthermore, we also updated our terms of service that include our commitments to everyone using Facebook. We explain the services we offer in language that's easier to read. We've also updated our Data Policy to better spell out what data we collect and how we use it in Facebook, Instagram, Messenger, and other products.

363. When will Facebook switch to OPT-IN instead of OPT-OUT?

We believe that it's important to communicate with people about the information that we collect and how people can control it. As explained in our Data Policy, we collect three basic categories of data about people:

- (1) data about things people do and share (and who they connect with) on our services;
- (2) data about the devices people use to access our services; and
- (3) data we receive from partners, including the websites and apps that use our business tools.

We collect information about the people, Pages, accounts, hashtags, and groups users are connected to and how they interact with them across our Products, such as people a user communicates with the most or groups users are part of. We also collect contact information if they choose to upload, sync, or import it from a device (such as an address book or call log or SMS log history), which we use for things like helping them and others find people they may know.

The data we use to show ads to people depends on the data we have received from people. For people who are new to Facebook, we may have minimal data that we can use. For people who have used our services for longer, we likely have more data, but the amount of data will depend on the nature of that use and how they have used our controls. Any person can see each of the specific interests we maintain about them for advertising by visiting Ads Preferences, which lets people see what interests we use to choose ads for them—and to edit or delete these interests. We also provide more detailed information about how we use data to decide what ads to show to people in our "About Facebook Ads" page, at https://www.facebook.com/ads/about. And, we do not sell people's information to anyone, and we never will.

All users must expressly consent to Facebook's Terms and Data Policy when registering for Facebook. The Data Policy explains the kinds of information we collect, how we use this information, how we share this information, and how users can manage and delete information.

Facebook does not create profiles for people without a Facebook account, but we do receive some information from devices and browsers that may be used by non-users. For example:

- When people visit apps or websites that feature our technologies—like the Facebook Like or Comment button—our servers automatically log (i) standard browser or app records of the fact that a particular device or user visited the website or app (this connection to Facebook's servers occurs automatically when a person visits a website or app that contains our technologies, such as a Like button, and is an inherent function of Internet design); and (ii) any additional information the publisher of the app or website chooses to share with Facebook about the person's activities on that site (such as the fact that a purchase was made on the site). This is a standard feature of the Internet, and most websites and apps share this same information with multiple different third-parties whenever people visit their website or app. When the person visiting a website featuring Facebook's tools is not a registered Facebook user, Facebook does not have information identifying that individual, and it does not create profiles for this individual.

- We also may receive information about the device of a non-registered user if that user visits a part of Facebook that does not require people to log in—such as a public Facebook Page. The information we log when people visit our websites or apps is the same as described above and is the same information that any provider of an online service would receive.

- In addition, Facebook may receive some basic information about devices where Facebook apps are installed, including before people using those devices have registered for Facebook (such as when a user downloads a Facebook app, but has not yet created an

account, or if the app is preloaded on a given device). This device data includes things like device model, operating system, IP address, app version and device identifiers. We use this information to provide the right version of the app, help people who want to create accounts (for example, optimizing the registration flow for the specific device), retrieving bug fixes and measuring and improving app performance. We do not use this information to build profiles about non-registered users.

364. Why collect all this personal data from users such as real birthdays, real names, etc. if you weren't planning to monetize it in this fashion, sell it to others whether or not users wanted to share it? If that wasn't the plan from the beginning, why demand real personal information from users, no fake names, etc.?

A note: It's clear to me that using all that data was the whole point, no matter what Facebook claims. I think social media is disastrous for personal privacy and consider Facebook to always have been the worst offender. I will have nothing to do with it. I prophesied that this would happen years ago and no one I knew believed me. And now here we are. Of course it was foolish to put all that information online for strangers to see and take. The twitterverse has taken over reality. Go get 'em Anna!

We believe that it's important to communicate with people about the information that we collect and how people can control it. As explained in our Data Policy, we collect three basic categories of data about people:

- (1) data about things people do and share (and who they connect with) on our services;
- (2) data about the devices people use to access our services; and
- (3) data we receive from partners, including the websites and apps that use our business tools.

We collect information about the people, Pages, accounts, hashtags, and groups users are connected to and how they interact with them across our Products, such as people a user communicates with the most or groups users are part of. We also collect contact information if they choose to upload, sync, or import it from a device (such as an address book or call log or SMS log history), which we use for things like helping them and others find people they may know.

The data we use to show ads to people depends on the data we have received from people. For people who are new to Facebook, we may have minimal data that we can use. For people who have used our services for longer, we likely have more data, but the amount of data will depend on the nature of that use and how they have used our controls. Any person can see each of the specific interests we maintain about them for advertising by visiting Ads Preferences, which lets people see what interests we use to choose ads for them—and to edit or delete these interests. We also provide more detailed information about how we use data to decide what ads to show to people in our "About Facebook Ads" page, at https://www.facebook.com/ads/about. And, we do not sell people's information to anyone, and we never will.

All users must expressly consent to Facebook's Terms and Data Policy when registering for Facebook. The Data Policy explains the kinds of information we collect, how we use this information, how we share this information, and how users can manage and delete information.

Facebook does not create profiles for people without a Facebook account, but we do receive some information from devices and browsers that may be used by non-users. For example:

- When people visit apps or websites that feature our technologies—like the Facebook Like or Comment button—our servers automatically log (i) standard browser or app records of the fact that a particular device or user visited the website or app (this connection to Facebook's servers occurs automatically when a person visits a website or app that contains our technologies, such as a Like button, and is an inherent function of Internet design); and (ii) any additional information the publisher of the app or website chooses to share with Facebook about the person's activities on that site (such as the fact that a purchase was made on the site). This is a standard feature of the Internet, and most websites and apps share this same information with multiple different third-parties whenever people visit their website or app. When the person visiting a website featuring Facebook's tools is not a registered Facebook user, Facebook does not have information identifying that individual, and it does not create profiles for this individual.

- We also may receive information about the device of a non-registered user if that user visits a part of Facebook that does not require people to log in—such as a public Facebook Page. The information we log when people visit our websites or apps is the same as described above and is the same information that any provider of an online service would receive.

- In addition, Facebook may receive some basic information about devices where Facebook apps are installed, including before people using those devices have registered for Facebook (such as when a user downloads a Facebook app, but has not yet created an account, or if the app is preloaded on a given device). This device data includes things like device model, operating system, IP address, app version and device identifiers. We use this information to provide the right version of the app, help people who want to create accounts (for example, optimizing the registration flow for the specific device), retrieving bug fixes and measuring and improving app performance. We do not use this information to build profiles about non-registered users.

365. I was getting ads from NRA after I deleted them from my news feed. Is profit more important than our precious children and citizen's lives and privacy?

To build a secure product with extensive infrastructure that connects people wherever they live or whatever their income level, we need to make sure everyone can afford it. Advertising lets us keep Facebook free, which ensures it remains affordable for everyone. We also believe the ads you see across the Facebook family of apps and services should be useful and relevant to you. Users can't opt out of seeing ads altogether because selling ads is what keeps Facebook free, but they do have different options to control how their data can and can't be used to show them ads. They're all found in ad preferences, which allows users to turn off the

use of all data collected from partners off Facebook to target ads. Users can also decide which of their profile fields they want used for ad targeting in the Information section under "About you." Users can remove themselves from interests under "Your interests" and categories under "Your categories." And, we do not sell people's information to anyone, and we never will.

Facebook is committed to transparency for all ads, including ads with political content. Facebook believes that people should be able to easily understand why they are seeing ads, who paid for them, and what other ads those advertisers are running. As such, Facebook only allows authorized advertisers to run ads about elections or issues that are being debated across the country. In order to be authorized by Facebook, advertisers will need to confirm their identity and location. Furthermore, all political and issue ads will include a disclosure which reads: "Paid for by," and when users click on this disclosure they will be able to see details about the advertiser. Users will also be able to see an explanation of why they saw the particular ad. This is similar to the disclosure included on political TV advertisements. We just launched globally View Active Ads, a feature that will enable anyone to see all of the ads an advertiser is currently running by visiting the advertiser's Facebook Page.

366. Does he plan to change his business model of selling his customer data if so how?

We believe that it's important to communicate with people about the information that we collect and how people can control it. As explained in our Data Policy, we collect three basic categories of data about people:

- (1) data about things people do and share (and who they connect with) on our services;
- (2) data about the devices people use to access our services; and
- (3) data we receive from partners, including the websites and apps that use our business tools.

We collect information about the people, Pages, accounts, hashtags, and groups users are connected to and how they interact with them across our Products, such as people a user communicates with the most or groups users are part of. We also collect contact information if they choose to upload, sync, or import it from a device (such as an address book or call log or SMS log history), which we use for things like helping them and others find people they may know.

The data we use to show ads to people depends on the data we have received from people. For people who are new to Facebook, we may have minimal data that we can use. For people who have used our services for longer, we likely have more data, but the amount of data will depend on the nature of that use and how they have used our controls. Any person can see each of the specific interests we maintain about them for advertising by visiting Ads Preferences, which lets people see what interests we use to choose ads for them—and to edit or delete these interests. We also provide more detailed information about how we use data to decide what ads to show to people in our "About Facebook Ads" page, at https://www.facebook.com/ads/about. And, we do not sell people's information to anyone, and we never will.

All users must expressly consent to Facebook's Terms and Data Policy when registering for Facebook. The Data Policy explains the kinds of information we collect, how we use this information, how we share this information, and how users can manage and delete information.

Facebook does not create profiles for people without a Facebook account, but we do receive some information from devices and browsers that may be used by non-users. For example:

- When people visit apps or websites that feature our technologies—like the Facebook Like or Comment button—our servers automatically log (i) standard browser or app records of the fact that a particular device or user visited the website or app (this connection to Facebook's servers occurs automatically when a person visits a website or app that contains our technologies, such as a Like button, and is an inherent function of Internet design); and (ii) any additional information the publisher of the app or website chooses to share with Facebook about the person's activities on that site (such as the fact that a purchase was made on the site). This is a standard feature of the Internet, and most websites and apps share this same information with multiple different third-parties whenever people visit their website or app. When the person visiting a website featuring Facebook's tools is not a registered Facebook user, Facebook does not have information identifying that individual, and it does not create profiles for this individual.

- We also may receive information about the device of a non-registered user if that user visits a part of Facebook that does not require people to log in—such as a public Facebook Page. The information we log when people visit our websites or apps is the same as described above and is the same information that any provider of an online service would receive.

- In addition, Facebook may receive some basic information about devices where Facebook apps are installed, including before people using those devices have registered for Facebook (such as when a user downloads a Facebook app, but has not yet created an account, or if the app is preloaded on a given device). This device data includes things like device model, operating system, IP address, app version and device identifiers. We use this information to provide the right version of the app, help people who want to create accounts (for example, optimizing the registration flow for the specific device), retrieving bug fixes and measuring and improving app performance. We do not use this information to build profiles about non-registered users.

367. Flow did they allow advertisers to market to people's bigotries?

To build a secure product with extensive infrastructure that connects people wherever they live or whatever their income level, we need to make sure everyone can afford it. Advertising lets us keep Facebook free, which ensures it remains affordable for everyone. We also believe the ads you see across the Facebook family of apps and services should be useful and relevant to you. Users can't opt out of seeing ads altogether because selling ads is what keeps Facebook free, but they do have different options to control how their data can and can't be used to show them ads. They're all found in ad preferences, which allows users to turn off the use of all data collected from partners off Facebook to target ads. Users can also decide which of

their profile fields they want used for ad targeting in the Information section under "About you." Users can remove themselves from interests under "Your interests" and categories under "Your categories." And, we do not sell people's information to anyone, and we never will.

Facebook is committed to transparency for all ads, including ads with political content. Facebook believes that people should be able to easily understand why they are seeing ads, who paid for them, and what other ads those advertisers are running. As such, Facebook only allows authorized advertisers to run ads about elections or issues that are being debated across the country. In order to be authorized by Facebook, advertisers will need to confirm their identity and location. Furthermore, all political and issue ads will include a disclosure which reads: "Paid for by," and when users click on this disclosure they will be able to see details about the advertiser. Users will also be able to see an explanation of why they saw the particular ad. This is similar to the disclosure included on political TV advertisements. We just launched globally View Active Ads, a feature that will enable anyone to see all of the ads an advertiser is currently running by visiting the advertiser's Facebook Page.

368. How do you intend to keep FaceBook profitable if you are no longer selling access to data about your members to businesses interested in that data?

We believe that it's important to communicate with people about the information that we collect and how people can control it. As explained in our Data Policy, we collect three basic categories of data about people:

- (1) data about things people do and share (and who they connect with) on our services;
- (2) data about the devices people use to access our services; and
- (3) data we receive from partners, including the websites and apps that use our business tools.

We collect information about the people, Pages, accounts, hashtags, and groups users are connected to and how they interact with them across our Products, such as people a user communicates with the most or groups users are part of. We also collect contact information if they choose to upload, sync, or import it from a device (such as an address book or call log or SMS log history), which we use for things like helping them and others find people they may know.

The data we use to show ads to people depends on the data we have received from people. For people who are new to Facebook, we may have minimal data that we can use. For people who have used our services for longer, we likely have more data, but the amount of data will depend on the nature of that use and how they have used our controls. Any person can see each of the specific interests we maintain about them for advertising by visiting Ads Preferences, which lets people see what interests we use to choose ads for them—and to edit or delete these interests. We also provide more detailed information about how we use data to decide what ads to show to people in our "About Facebook Ads" page, at https://www.facebook.com/ads/about. And, we do not sell people's information to anyone, and we never will.

All users must expressly consent to Facebook's Terms and Data Policy when registering for Facebook. The Data Policy explains the kinds of information we collect, how we use this information, how we share this information, and how users can manage and delete information.

Facebook does not create profiles for people without a Facebook account, but we do receive some information from devices and browsers that may be used by non-users. For example:

- When people visit apps or websites that feature our technologies—like the Facebook Like or Comment button—our servers automatically log (i) standard browser or app records of the fact that a particular device or user visited the website or app (this connection to Facebook's servers occurs automatically when a person visits a website or app that contains our technologies, such as a Like button, and is an inherent function of Internet design); and (ii) any additional information the publisher of the app or website chooses to share with Facebook about the person's activities on that site (such as the fact that a purchase was made on the site). This is a standard feature of the Internet, and most websites and apps share this same information with multiple different third-parties whenever people visit their website or app. When the person visiting a website featuring Facebook's tools is not a registered Facebook user, Facebook does not have information identifying that individual, and it does not create profiles for this individual.

- We also may receive information about the device of a non-registered user if that user visits a part of Facebook that does not require people to log in—such as a public Facebook Page. The information we log when people visit our websites or apps is the same as described above and is the same information that any provider of an online service would receive.

- In addition, Facebook may receive some basic information about devices where Facebook apps are installed, including before people using those devices have registered for Facebook (such as when a user downloads a Facebook app, but has not yet created an account, or if the app is preloaded on a given device). This device data includes things like device model, operating system, IP address, app version and device identifiers. We use this information to provide the right version of the app, help people who want to create accounts (for example, optimizing the registration flow for the specific device), retrieving bug fixes and measuring and improving app performance. We do not use this information to build profiles about non-registered users.

369. (1) From FB's perspective, what are the principles underlying the balancing act of protecting data privacy vs. sharing data to advance company's priorities in growth and to advance pro-social initiatives?
(2) What metrics does FB use to measure its effectiveness in safeguarding user data? How does FB benchmark itself in comparison to other tech companies? What standard / target measures does FB hold itself up to?

We believe everyone deserves good privacy controls. A user owns the information they share on Facebook. This means they decide what they share and who they share it with on Facebook, and they can change their mind. We require websites and apps who use our tools to

tell users they're collecting and sharing their information with us, and to get users' permission to do so.

Everyone has the right to expect strong protections for their information. We also need to do our part to help keep our community safe, in a way that's consistent with people's privacy expectations. We've recently announced several steps to give people more control over their privacy, including a new Privacy Shortcuts tool that we're rolling out now to give people information about how to control their information, including choosing who can see what they post and adding protections like two-factor authentication to their account. People can learn more about how to protect their privacy in our updated Data Policy and in our Privacy Basics feature (https://www.facebook.com/about/basics).

We are in the process of investigating every app that had access to a large amount of information before we changed our Platform in 2014. The investigation process is in full swing. We have large teams of internal and external experts working hard to investigate these apps as quickly as possible. As of early June 2018, thousands of apps have been investigated and around 200 apps have been suspended—pending a thorough investigation into whether they did in fact misuse any data. Where we find evidence that these or other apps did misuse data, we will ban them and let people know.

Facebook is generally not opposed to regulation but wants to ensure it is the right regulation. The issues facing the industry are complex, multi-faceted, and affect an important part of peoples' lives. As such, Facebook is absolutely committed to working with regulators, like Congress, to craft the right regulations. Facebook would be happy to review any proposed legislation and provide comments.

370. Was this all part of the strategy to accumulate monetary wealth by selling users' personal information to anyone willing to pay regardless of their intentions?

We believe that it's important to communicate with people about the information that we collect and how people can control it. As explained in our Data Policy, we collect three basic categories of data about people:

- (1) data about things people do and share (and who they connect with) on our services;
- (2) data about the devices people use to access our services; and
- (3) data we receive from partners, including the websites and apps that use our business tools.

We collect information about the people, Pages, accounts, hashtags, and groups users are connected to and how they interact with them across our Products, such as people a user communicates with the most or groups users are part of. We also collect contact information if they choose to upload, sync, or import it from a device (such as an address book or call log or SMS log history), which we use for things like helping them and others find people they may know.

The data we use to show ads to people depends on the data we have received from people. For people who are new to Facebook, we may have minimal data that we can use. For people who have used our services for longer, we likely have more data, but the amount of data will depend on the nature of that use and how they have used our controls. Any person can see each of the specific interests we maintain about them for advertising by visiting Ads Preferences, which lets people see what interests we use to choose ads for them—and to edit or delete these interests. We also provide more detailed information about how we use data to decide what ads to show to people in our "About Facebook Ads" page, at https://www.facebook.com/ads/about. And, we do not sell people's information to anyone, and we never will.

All users must expressly consent to Facebook's Terms and Data Policy when registering for Facebook. The Data Policy explains the kinds of information we collect, how we use this information, how we share this information, and how users can manage and delete information.

Facebook does not create profiles for people without a Facebook account, but we do receive some information from devices and browsers that may be used by non-users. For example:

- When people visit apps or websites that feature our technologies—like the Facebook Like or Comment button—our servers automatically log (i) standard browser or app records of the fact that a particular device or user visited the website or app (this connection to Facebook's servers occurs automatically when a person visits a website or app that contains our technologies, such as a Like button, and is an inherent function of Internet design); and (ii) any additional information the publisher of the app or website chooses to share with Facebook about the person's activities on that site (such as the fact that a purchase was made on the site). This is a standard feature of the Internet, and most websites and apps share this same information with multiple different third-parties whenever people visit their website or app. When the person visiting a website featuring Facebook's tools is not a registered Facebook user, Facebook does not have information identifying that individual, and it does not create profiles for this individual.

- We also may receive information about the device of a non-registered user if that user visits a part of Facebook that does not require people to log in—such as a public Facebook Page. The information we log when people visit our websites or apps is the same as described above and is the same information that any provider of an online service would receive.

- In addition, Facebook may receive some basic information about devices where Facebook apps are installed, including before people using those devices have registered for Facebook (such as when a user downloads a Facebook app, but has not yet created an account, or if the app is preloaded on a given device). This device data includes things like device model, operating system, IP address, app version and device identifiers. We use this information to provide the right version of the app, help people who want to create accounts (for example, optimizing the registration flow for the specific device), retrieving bug fixes and measuring and improving app performance. We do not use this information to build profiles about non-registered users.

371. What other companies and applications have had access to user's data over the last 10 years?

To build a secure product with extensive infrastructure that connects people wherever they live or whatever their income level, we need to make sure everyone can afford it. Advertising lets us keep Facebook free, which ensures it remains affordable for everyone. We also believe the ads you see across the Facebook family of apps and services should be useful and relevant to you. Users can't opt out of seeing ads altogether because selling ads is what keeps Facebook free, but they do have different options to control how their data can and can't be used to show them ads. They're all found in ad preferences, which allows users to turn off the use of all data collected from partners off Facebook to target ads. Users can also decide which of their profile fields they want used for ad targeting in the Information section under "About you." Users can remove themselves from interests under "Your interests" and categories under "Your categories." And, we do not sell people's information to anyone, and we never will.

Facebook is committed to transparency for all ads, including ads with political content. Facebook believes that people should be able to easily understand why they are seeing ads, who paid for them, and what other ads those advertisers are running. As such, Facebook only allows authorized advertisers to run ads about elections or issues that are being debated across the country. In order to be authorized by Facebook, advertisers will need to confirm their identity and location. Furthermore, all political and issue ads will include a disclosure which reads: "Paid for by," and when users click on this disclosure they will be able to see details about the advertiser. Users will also be able to see an explanation of why they saw the particular ad. This is similar to the disclosure included on political TV advertisements. We just launched globally View Active Ads, a feature that will enable anyone to see all of the ads an advertiser is currently running by visiting the advertiser's Facebook Page.

372. How does Facebook earn revenue? Is it selling user data?

We believe that it's important to communicate with people about the information that we collect and how people can control it. As explained in our Data Policy, we collect three basic categories of data about people:

- (1) data about things people do and share (and who they connect with) on our services;
- (2) data about the devices people use to access our services; and
- (3) data we receive from partners, including the websites and apps that use our business tools.

We collect information about the people, Pages, accounts, hashtags, and groups users are connected to and how they interact with them across our Products, such as people a user communicates with the most or groups users are part of. We also collect contact information if they choose to upload, sync, or import it from a device (such as an address book or call log or SMS log history), which we use for things like helping them and others find people they may know.

The data we use to show ads to people depends on the data we have received from people. For people who are new to Facebook, we may have minimal data that we can use. For people who have used our services for longer, we likely have more data, but the amount of data will depend on the nature of that use and how they have used our controls. Any person can see each of the specific interests we maintain about them for advertising by visiting Ads Preferences, which lets people see what interests we use to choose ads for them—and to edit or delete these interests. We also provide more detailed information about how we use data to decide what ads to show to people in our "About Facebook Ads" page, at https://www.facebook.com/ads/about. And, we do not sell people's information to anyone, and we never will.

All users must expressly consent to Facebook's Terms and Data Policy when registering for Facebook. The Data Policy explains the kinds of information we collect, how we use this information, how we share this information, and how users can manage and delete information.

Facebook does not create profiles for people without a Facebook account, but we do receive some information from devices and browsers that may be used by non-users. For example:

- When people visit apps or websites that feature our technologies—like the Facebook Like or Comment button—our servers automatically log (i) standard browser or app records of the fact that a particular device or user visited the website or app (this connection to Facebook's servers occurs automatically when a person visits a website or app that contains our technologies, such as a Like button, and is an inherent function of Internet design); and (ii) any additional information the publisher of the app or website chooses to share with Facebook about the person's activities on that site (such as the fact that a purchase was made on the site). This is a standard feature of the Internet, and most websites and apps share this same information with multiple different third-parties whenever people visit their website or app. When the person visiting a website featuring Facebook's tools is not a registered Facebook user, Facebook does not have information identifying that individual, and it does not create profiles for this individual.

- We also may receive information about the device of a non-registered user if that user visits a part of Facebook that does not require people to log in—such as a public Facebook Page. The information we log when people visit our websites or apps is the same as described above and is the same information that any provider of an online service would receive.

- In addition, Facebook may receive some basic information about devices where Facebook apps are installed, including before people using those devices have registered for Facebook (such as when a user downloads a Facebook app, but has not yet created an account, or if the app is preloaded on a given device). This device data includes things like device model, operating system, IP address, app version and device identifiers. We use this information to provide the right version of the app, help people who want to create accounts (for example, optimizing the registration flow for the specific device), retrieving bug fixes and measuring and improving app performance. We do not use this information to build profiles about non-registered users.

373. Is it accurate to say that a Facebook user is really the product and that Facebook cannot exist without monetizing the data of its users?

We believe that it's important to communicate with people about the information that we collect and how people can control it. As explained in our Data Policy, we collect three basic categories of data about people:

- (1) data about things people do and share (and who they connect with) on our services;
- (2) data about the devices people use to access our services; and
- (3) data we receive from partners, including the websites and apps that use our business tools.

We collect information about the people, Pages, accounts, hashtags, and groups users are connected to and how they interact with them across our Products, such as people a user communicates with the most or groups users are part of. We also collect contact information if they choose to upload, sync, or import it from a device (such as an address book or call log or SMS log history), which we use for things like helping them and others find people they may know.

The data we use to show ads to people depends on the data we have received from people. For people who are new to Facebook, we may have minimal data that we can use. For people who have used our services for longer, we likely have more data, but the amount of data will depend on the nature of that use and how they have used our controls. Any person can see each of the specific interests we maintain about them for advertising by visiting Ads Preferences, which lets people see what interests we use to choose ads for them—and to edit or delete these interests. We also provide more detailed information about how we use data to decide what ads to show to people in our "About Facebook Ads" page, at https://www.facebook.com/ads/about. And, we do not sell people's information to anyone, and we never will.

All users must expressly consent to Facebook's Terms and Data Policy when registering for Facebook. The Data Policy explains the kinds of information we collect, how we use this information, how we share this information, and how users can manage and delete information.

Facebook does not create profiles for people without a Facebook account, but we do receive some information from devices and browsers that may be used by non-users. For example:

- When people visit apps or websites that feature our technologies—like the Facebook Like or Comment button—our servers automatically log (i) standard browser or app records of the fact that a particular device or user visited the website or app (this connection to Facebook's servers occurs automatically when a person visits a website or app that contains our technologies, such as a Like button, and is an inherent function of Internet design); and (ii) any additional information the publisher of the app or website chooses to share with Facebook about the person's activities on that site (such as the fact that a purchase was made on the site). This is a standard feature of the Internet, and most

websites and apps share this same information with multiple different third-parties whenever people visit their website or app. When the person visiting a website featuring Facebook's tools is not a registered Facebook user, Facebook does not have information identifying that individual, and it does not create profiles for this individual.

- We also may receive information about the device of a non-registered user if that user visits a part of Facebook that does not require people to log in—such as a public Facebook Page. The information we log when people visit our websites or apps is the same as described above and is the same information that any provider of an online service would receive.

- In addition, Facebook may receive some basic information about devices where Facebook apps are installed, including before people using those devices have registered for Facebook (such as when a user downloads a Facebook app, but has not yet created an account, or if the app is preloaded on a given device). This device data includes things like device model, operating system, IP address, app version and device identifiers. We use this information to provide the right version of the app, help people who want to create accounts (for example, optimizing the registration flow for the specific device), retrieving bug fixes and measuring and improving app performance. We do not use this information to build profiles about non-registered users.

374. Which third parties have accessed Facebook, which data was obtained, and how did they obtain access?

Facebook's policies regarding third-party usage of its platform technologies have prohibited—and continue to prohibit—third-party app developers from selling or licensing user data obtained from Facebook and from sharing any user data obtained from Facebook with any ad network, data broker or other advertising or monetization-related service.

We use a variety of tools to enforce Facebook policies against violating parties, including developers. We review tens of thousands of apps per year and regularly disapprove noncompliant apps as part of our proactive review process. We also use tools like cease and desist letters, account suspensions, letter agreements, and civil litigation. For example, since 2006, Facebook has sent over 1,150 cease-and-desist letters to over 1,600 targets. In 2017, we took action against about 370,000 apps, ranging from imposing certain restrictions to removal of the app from the platform. Moreover, we have required parties who have procured our data without authorization to delete that data. We have invested significant resources in these efforts.

Recently, we announced a number of additional steps we're taking to address concerns raised by Kogan's app.

- **Review our platform.** We will investigate all apps that had access to large amounts of data before the platform changes we announced in 2014, and we will audit any app where we identify suspicious activity. If we identify misuses of data, we'll take immediate action, including banning the app from our platform and pursuing legal action if appropriate.

- **Tell people about data misuse.** We will tell people about apps that have misused their data. This includes building a way for people to know if their data might have been accessed via the app. Moving forward, if we remove an app, we will tell people.

- **Turn off access for unused apps.** If someone has not used an app within the last three months, we will turn off the app's access to their data.

- **Restrict Facebook Login data.** We are changing Login, so that the only data that an app can request without app review will include name, profile photo, and email address. Requesting any other data will require approval from Facebook. We will also no longer allow apps to ask for access to information like religious or political views, relationship status and details, custom friends lists, education and work history, fitness activity, book reading and music listening activity, news reading, video watch activity, and games activity. We will encourage people to manage the apps they use. We already show people what apps their accounts are connected to and allow them to control what data they've permitted those apps to use. But we're making it easier for people to see what apps they use and the information they have shared with those apps.

- **Reward people who find vulnerabilities.** We launched the Data Abuse Bounty program so that people can report to us any misuses of data by app developers.

- **Update our policies.** We have updated our terms and Data Policy to explain how we use data and how data is shared with app developers.

375. How revenue much per FB user would be lost by not sharing user data? How much market cap?

We believe everyone deserves good privacy controls. A user owns the information they share on Facebook. This means they decide what they share and who they share it with on Facebook, and they can change their mind. We require websites and apps who use our tools to tell users they're collecting and sharing their information with us, and to get users' permission to do so.

Everyone has the right to expect strong protections for their information. We also need to do our part to help keep our community safe, in a way that's consistent with people's privacy expectations. We've recently announced several steps to give people more control over their privacy, including a new Privacy Shortcuts tool that we're rolling out now to give people information about how to control their information, including choosing who can see what they post and adding protections like two-factor authentication to their account. People can learn more about how to protect their privacy in our updated Data Policy and in our Privacy Basics feature (https://www.facebook.com/about/basics).

We are in the process of investigating every app that had access to a large amount of information before we changed our Platform in 2014. The investigation process is in full swing. We have large teams of internal and external experts working hard to investigate these apps as quickly as possible. As of early June 2018, thousands of apps have been investigated and around 200 apps have been suspended—pending a thorough investigation into whether they did in fact

misuse any data. Where we find evidence that these or other apps did misuse data, we will ban them and let people know.

Facebook is generally not opposed to regulation but wants to ensure it is the right regulation. The issues facing the industry are complex, multi-faceted, and affect an important part of peoples' lives. As such, Facebook is absolutely committed to working with regulators, like Congress, to craft the right regulations. Facebook would be happy to review any proposed legislation and provide comments.

376. Was the Facebook business model, originally conceived to offer up user data to sell to advertisers?

To build a secure product with extensive infrastructure that connects people wherever they live or whatever their income level, we need to make sure everyone can afford it. Advertising lets us keep Facebook free, which ensures it remains affordable for everyone. We also believe the ads you see across the Facebook family of apps and services should be useful and relevant to you. Users can't opt out of seeing ads altogether because selling ads is what keeps Facebook free, but they do have different options to control how their data can and can't be used to show them ads. They're all found in ad preferences, which allows users to turn off the use of all data collected from partners off Facebook to target ads. Users can also decide which of their profile fields they want used for ad targeting in the Information section under "About you." Users can remove themselves from interests under "Your interests" and categories under "Your categories." And, we do not sell people's information to anyone, and we never will.

Facebook is committed to transparency for all ads, including ads with political content. Facebook believes that people should be able to easily understand why they are seeing ads, who paid for them, and what other ads those advertisers are running. As such, Facebook only allows authorized advertisers to run ads about elections or issues that are being debated across the country. In order to be authorized by Facebook, advertisers will need to confirm their identity and location. Furthermore, all political and issue ads will include a disclosure which reads: "Paid for by," and when users click on this disclosure they will be able to see details about the advertiser. Users will also be able to see an explanation of why they saw the particular ad. This is similar to the disclosure included on political TV advertisements. We just launched globally View Active Ads, a feature that will enable anyone to see all of the ads an advertiser is currently running by visiting the advertiser's Facebook Page.

377. How many other organizations like Cambridge Analytical have paid Facebook for our profile info?

We believe everyone deserves good privacy controls. A user owns the information they share on Facebook. This means they decide what they share and who they share it with on Facebook, and they can change their mind. We require websites and apps who use our tools to tell users they're collecting and sharing their information with us, and to get users' permission to do so.

Everyone has the right to expect strong protections for their information. We also need to do our part to help keep our community safe, in a way that's consistent with people's privacy

expectations. We've recently announced several steps to give people more control over their privacy, including a new Privacy Shortcuts tool that we're rolling out now to give people information about how to control their information, including choosing who can see what they post and adding protections like two-factor authentication to their account. People can learn more about how to protect their privacy in our updated Data Policy and in our Privacy Basics feature (https://www.facebook.com/about/basics).

We are in the process of investigating every app that had access to a large amount of information before we changed our Platform in 2014. The investigation process is in full swing. We have large teams of internal and external experts working hard to investigate these apps as quickly as possible. As of early June 2018, thousands of apps have been investigated and around 200 apps have been suspended—pending a thorough investigation into whether they did in fact misuse any data. Where we find evidence that these or other apps did misuse data, we will ban them and let people know.

Facebook is generally not opposed to regulation but wants to ensure it is the right regulation. The issues facing the industry are complex, multi-faceted, and affect an important part of peoples' lives. As such, Facebook is absolutely committed to working with regulators, like Congress, to craft the right regulations. Facebook would be happy to review any proposed legislation and provide comments.

378. To what extent would restrictions on access to users' data reduce Facebook's profitability?

We believe that it's important to communicate with people about the information that we collect and how people can control it. As explained in our Data Policy, we collect three basic categories of data about people:

- (1) data about things people do and share (and who they connect with) on our services;
- (2) data about the devices people use to access our services; and
- (3) data we receive from partners, including the websites and apps that use our business tools.

We collect information about the people, Pages, accounts, hashtags, and groups users are connected to and how they interact with them across our Products, such as people a user communicates with the most or groups users are part of. We also collect contact information if they choose to upload, sync, or import it from a device (such as an address book or call log or SMS log history), which we use for things like helping them and others find people they may know.

The data we use to show ads to people depends on the data we have received from people. For people who are new to Facebook, we may have minimal data that we can use. For people who have used our services for longer, we likely have more data, but the amount of data will depend on the nature of that use and how they have used our controls. Any person can see each of the specific interests we maintain about them for advertising by visiting Ads Preferences,

which lets people see what interests we use to choose ads for them—and to edit or delete these interests. We also provide more detailed information about how we use data to decide what ads to show to people in our "About Facebook Ads" page, at https://www.facebook.com/ads/about. And, we do not sell people's information to anyone, and we never will.

All users must expressly consent to Facebook's Terms and Data Policy when registering for Facebook. The Data Policy explains the kinds of information we collect, how we use this information, how we share this information, and how users can manage and delete information.

Facebook does not create profiles for people without a Facebook account, but we do receive some information from devices and browsers that may be used by non-users. For example:

- When people visit apps or websites that feature our technologies—like the Facebook Like or Comment button—our servers automatically log (i) standard browser or app records of the fact that a particular device or user visited the website or app (this connection to Facebook's servers occurs automatically when a person visits a website or app that contains our technologies, such as a Like button, and is an inherent function of Internet design); and (ii) any additional information the publisher of the app or website chooses to share with Facebook about the person's activities on that site (such as the fact that a purchase was made on the site). This is a standard feature of the Internet, and most websites and apps share this same information with multiple different third-parties whenever people visit their website or app. When the person visiting a website featuring Facebook's tools is not a registered Facebook user, Facebook does not have information identifying that individual, and it does not create profiles for this individual.

- We also may receive information about the device of a non-registered user if that user visits a part of Facebook that does not require people to log in—such as a public Facebook Page. The information we log when people visit our websites or apps is the same as described above and is the same information that any provider of an online service would receive.

- In addition, Facebook may receive some basic information about devices where Facebook apps are installed, including before people using those devices have registered for Facebook (such as when a user downloads a Facebook app, but has not yet created an account, or if the app is preloaded on a given device). This device data includes things like device model, operating system, IP address, app version and device identifiers. We use this information to provide the right version of the app, help people who want to create accounts (for example, optimizing the registration flow for the specific device), retrieving bug fixes and measuring and improving app performance. We do not use this information to build profiles about non-registered users.

379. Would he be willing to give up his business model in the interest of protecting individual privacy?

We believe everyone deserves good privacy controls. A user owns the information they share on Facebook. This means they decide what they share and who they share it with on

Facebook, and they can change their mind. We require websites and apps who use our tools to tell users they're collecting and sharing their information with us, and to get users' permission to do so.

Everyone has the right to expect strong protections for their information. We also need to do our part to help keep our community safe, in a way that's consistent with people's privacy expectations. We've recently announced several steps to give people more control over their privacy, including a new Privacy Shortcuts tool that we're rolling out now to give people information about how to control their information, including choosing who can see what they post and adding protections like two-factor authentication to their account. People can learn more about how to protect their privacy in our updated Data Policy and in our Privacy Basics feature (https://www.facebook.com/about/basics).

We are in the process of investigating every app that had access to a large amount of information before we changed our Platform in 2014. The investigation process is in full swing. We have large teams of internal and external experts working hard to investigate these apps as quickly as possible. As of early June 2018, thousands of apps have been investigated and around 200 apps have been suspended—pending a thorough investigation into whether they did in fact misuse any data. Where we find evidence that these or other apps did misuse data, we will ban them and let people know.

Facebook is generally not opposed to regulation but wants to ensure it is the right regulation. The issues facing the industry are complex, multi-faceted, and affect an important part of peoples' lives. As such, Facebook is absolutely committed to working with regulators, like Congress, to craft the right regulations. Facebook would be happy to review any proposed legislation and provide comments.

380. Would you consider offering users a paid subscription to your service rather than ransoming data?

To build a secure product with extensive infrastructure that connects people wherever they live or whatever their income level, we need to make sure everyone can afford it. Advertising lets us keep Facebook free, which ensures it remains affordable for everyone. We also believe the ads you see across the Facebook family of apps and services should be useful and relevant to you. Users can't opt out of seeing ads altogether because selling ads is what keeps Facebook free, but they do have different options to control how their data can and can't be used to show them ads. They're all found in ad preferences, which allows users to turn off the use of all data collected from partners off Facebook to target ads. Users can also decide which of their profile fields they want used for ad targeting in the Information section under "About you." Users can remove themselves from interests under "Your interests" and categories under "Your categories." And, we do not sell people's information to anyone, and we never will.

Facebook is committed to transparency for all ads, including ads with political content. Facebook believes that people should be able to easily understand why they are seeing ads, who paid for them, and what other ads those advertisers are running. As such, Facebook only allows authorized advertisers to run ads about elections or issues that are being debated across the country. In order to be authorized by Facebook, advertisers will need to confirm their identity

and location. Furthermore, all political and issue ads will include a disclosure which reads: "Paid for by," and when users click on this disclosure they will be able to see details about the advertiser. Users will also be able to see an explanation of why they saw the particular ad. This is similar to the disclosure included on political TV advertisements. We just launched globally View Active Ads, a feature that will enable anyone to see all of the ads an advertiser is currently running by visiting the advertiser's Facebook Page.

381. My question is, When FB says they allowed 3rd parties to access data, does that mean they sold our private user data? FB needs to be transparent and limited to the data they can release. The User needs regulated privacy. Why are they dealing with malicious 3rd parties?

We believe everyone deserves good privacy controls. A user owns the information they share on Facebook. This means they decide what they share and who they share it with on Facebook, and they can change their mind. We require websites and apps who use our tools to tell users they're collecting and sharing their information with us, and to get users' permission to do so.

Everyone has the right to expect strong protections for their information. We also need to do our part to help keep our community safe, in a way that's consistent with people's privacy expectations. We've recently announced several steps to give people more control over their privacy, including a new Privacy Shortcuts tool that we're rolling out now to give people information about how to control their information, including choosing who can see what they post and adding protections like two-factor authentication to their account. People can learn more about how to protect their privacy in our updated Data Policy and in our Privacy Basics feature (https://www.facebook.com/about/basics).

We are in the process of investigating every app that had access to a large amount of information before we changed our Platform in 2014. The investigation process is in full swing. We have large teams of internal and external experts working hard to investigate these apps as quickly as possible. As of early June 2018, thousands of apps have been investigated and around 200 apps have been suspended—pending a thorough investigation into whether they did in fact misuse any data. Where we find evidence that these or other apps did misuse data, we will ban them and let people know.

Facebook is generally not opposed to regulation but wants to ensure it is the right regulation. The issues facing the industry are complex, multi-faceted, and affect an important part of peoples' lives. As such, Facebook is absolutely committed to working with regulators, like Congress, to craft the right regulations. Facebook would be happy to review any proposed legislation and provide comments.

382. **Once again privacy of FB users has been treated without high regard. This is not first instance. Why should we believe anything you will say about changing attitude, adherence and respect? Note: in the past FB has made system changes and done such things as putting default two less privacy settings as an example. I believe there have been other instances of privacy not being taken seriously. It is now a pattern. This CEO has a flippant attitude towards respect for others as customers.**

We recognize that we have made mistakes, and we are committed to learning from this experience to secure our platform further and make our community safer for everyone going forward. As our CEO Mark Zuckerberg has said, when you are building something unprecedented like Facebook, there are going to be mistakes. What people should hold us accountable for is learning from the mistakes and continually doing better—and, at the end of the day, making sure that we're building things that people like and that make their lives better.

Particularly in the past few months, we've realized that we need to take a broader view of our responsibility to our community. Part of that effort is continuing our ongoing efforts to identify ways that we can improve our privacy practices. We've heard loud and clear that privacy settings and other important tools are too hard to find and that we must do more to keep people informed. So, we're taking additional steps to put people more in control of their privacy. For instance, we redesigned our entire settings menu on mobile devices from top to bottom to make things easier to find. We also created a new Privacy Shortcuts in a menu where users can control their data in just a few taps, with clearer explanations of how our controls work. The experience is now clearer, more visual, and easy-to-find. Furthermore, we also updated our terms of service that include our commitments to everyone using Facebook. We explain the services we offer in language that's easier to read. We've also updated our Data Policy to better spell out what data we collect and how we use it in Facebook, Instagram, Messenger, and other products.

383. You were informed by employees in 2010-2011 that Facebook was not auditing what was being done with it.

As discussed with your staff, this question is not germane to the hearing.

384. What is Facebook's responsibility to its customers and users?

We believe everyone deserves good privacy controls. A user owns the information they share on Facebook. This means they decide what they share and who they share it with on Facebook, and they can change their mind. We require websites and apps who use our tools to tell users they're collecting and sharing their information with us, and to get users' permission to do so.

Everyone has the right to expect strong protections for their information. We also need to do our part to help keep our community safe, in a way that's consistent with people's privacy expectations. We've recently announced several steps to give people more control over their privacy, including a new Privacy Shortcuts tool that we're rolling out now to give people information about how to control their information, including choosing who can see what they post and adding protections like two-factor authentication to their account. People can learn more about how to protect their privacy in our updated Data Policy and in our Privacy Basics feature (https://www.facebook.com/about/basics).

We are in the process of investigating every app that had access to a large amount of information before we changed our Platform in 2014. The investigation process is in full swing. We have large teams of internal and external experts working hard to investigate these apps as quickly as possible. As of early June 2018, thousands of apps have been investigated and around 200 apps have been suspended—pending a thorough investigation into whether they did in fact

misuse any data. Where we find evidence that these or other apps did misuse data, we will ban them and let people know.

Facebook is generally not opposed to regulation but wants to ensure it is the right regulation. The issues facing the industry are complex, multi-faceted, and affect an important part of peoples' lives. As such, Facebook is absolutely committed to working with regulators, like Congress, to craft the right regulations. Facebook would be happy to review any proposed legislation and provide comments.

385. Did you oversee the terms and conditions associated with the "Facebook Messenger" phone application? If so, were you aware that Facebook essentially stole the information of people without these individuals not signing the terms and agreements?

We believe that it's important to communicate with people about the information that we collect and how people can control it. As explained in our Data Policy, we collect three basic categories of data about people:

- (1) data about things people do and share (and who they connect with) on our services;
- (2) data about the devices people use to access our services; and
- (3) data we receive from partners, including the websites and apps that use our business tools.

We collect information about the people, Pages, accounts, hashtags, and groups users are connected to and how they interact with them across our Products, such as people a user communicates with the most or groups users are part of. We also collect contact information if they choose to upload, sync, or import it from a device (such as an address book or call log or SMS log history), which we use for things like helping them and others find people they may know.

The data we use to show ads to people depends on the data we have received from people. For people who are new to Facebook, we may have minimal data that we can use. For people who have used our services for longer, we likely have more data, but the amount of data will depend on the nature of that use and how they have used our controls. Any person can see each of the specific interests we maintain about them for advertising by visiting Ads Preferences, which lets people see what interests we use to choose ads for them—and to edit or delete these interests. We also provide more detailed information about how we use data to decide what ads to show to people in our "About Facebook Ads" page, at https://www.facebook.com/ads/about. And, we do not sell people's information to anyone, and we never will.

All users must expressly consent to Facebook's Terms and Data Policy when registering for Facebook. The Data Policy explains the kinds of information we collect, how we use this information, how we share this information, and how users can manage and delete information.

Facebook does not create profiles for people without a Facebook account, but we do receive some information from devices and browsers that may be used by non-users. For example:

- When people visit apps or websites that feature our technologies—like the Facebook Like or Comment button—our servers automatically log (i) standard browser or app records of the fact that a particular device or user visited the website or app (this connection to Facebook's servers occurs automatically when a person visits a website or app that contains our technologies, such as a Like button, and is an inherent function of Internet design); and (ii) any additional information the publisher of the app or website chooses to share with Facebook about the person's activities on that site (such as the fact that a purchase was made on the site). This is a standard feature of the Internet, and most websites and apps share this same information with multiple different third-parties whenever people visit their website or app. When the person visiting a website featuring Facebook's tools is not a registered Facebook user, Facebook does not have information identifying that individual, and it does not create profiles for this individual.

- We also may receive information about the device of a non-registered user if that user visits a part of Facebook that does not require people to log in—such as a public Facebook Page. The information we log when people visit our websites or apps is the same as described above and is the same information that any provider of an online service would receive.

- In addition, Facebook may receive some basic information about devices where Facebook apps are installed, including before people using those devices have registered for Facebook (such as when a user downloads a Facebook app, but has not yet created an account, or if the app is preloaded on a given device). This device data includes things like device model, operating system, IP address, app version and device identifiers. We use this information to provide the right version of the app, help people who want to create accounts (for example, optimizing the registration flow for the specific device), retrieving bug fixes and measuring and improving app performance. We do not use this information to build profiles about non-registered users.

386. How does fake news go viral and how does Facebook decide what people see or don't see?

We want Facebook to be a place where people can discover more news, information, and perspectives, and we are working to build products that help to that. Through our News Feed algorithm, we also work hard to actively reduce the distribution of clickbait, sensationalism, and misinformation, on the one hand, and to boost news and information from sources that are trusted, informative, and local, on the other hand.
We are focusing on four different strategies to address misinformation:

- **Strengthening enforcement of our authenticity policies.** We are investing heavily in new technology and hiring thousands more people to tackle the problem of inauthenticity on the platform. Fake accounts are often associated with false news, so this is an area that will have a huge impact on curbing the spread of inaccurate information.

- **Finding industry solutions.** All of us—from tech companies and media companies to newsrooms and classrooms—must work together to find industry solutions to strengthen the online news ecosystem and our own digital literacy. That's why we're collaborating with others who operate in this space. Last January, we announced The Facebook Journalism Project, an initiative that seeks to establish stronger ties between Facebook and the news industry. The project is focused on developing news products, providing training and tools for journalists, and working with publishers and educators on how we can equip people with the knowledge they need to be informed readers in the digital age. Since launching the Journalism Project, we've met with more than 2,600 publishers around the world to understand how they use our products and how we can make improvements to better support their needs.

- **Disrupting economic incentives.** When it comes to fighting false news, we've found that a lot of it is financially motivated. So, one of the most effective approaches is removing the economic incentives for those who traffic in inaccurate information. We've done things like block ads from pages that repeatedly share false news and significantly limit the distribution of web pages that deliver low quality web experiences.

- **Building new products.** We believe it's important to amplify the good effects of social media and mitigate the bad—to contribute to the diversity of ideas, information, and view points, while strengthening our common understanding.

    - We believe giving people more context can help them decide what to trust and what to share. The third-party fact-checking program we have developed uses reports from our community, along with other signals, to send stories to accredited third-party fact checking organizations. If the fact checking organizations identify a story as fake, we will suggest related articles in News Feed to show people different points of view, including information from fact checkers. Stories that have been disputed may also appear lower in News Feed. Our own data analytics show that a false rating from one of our fact checking partners reduces future impressions on Facebook by 80 percent.

    - We're also testing Article Context as a way of giving people more information about the material they're reading on Facebook. Since we launched this test, some of the articles people see in News Feed will feature an "i" icon that allows them to access more information at the tap of a button. The information we surface is pulled from across the internet, and includes things like the publisher's Wikipedia entry, trending articles or related articles about the topic, and information about how the article is being shared on Facebook. In some cases, if that information is unavailable, we will let people know since that can also be helpful context.

387. What specific steps are you taking to protect Facebook accounts from disinformation and propaganda?

We want Facebook to be a place where people can discover more news, information, and perspectives, and we are working to build products that help to that. Through our News Feed algorithm, we also work hard to actively reduce the distribution of clickbait, sensationalism, and

misinformation, on the one hand, and to boost news and information from sources that are trusted, informative, and local, on the other hand.
We are focusing on four different strategies to address misinformation:

- **Strengthening enforcement of our authenticity policies.** We are investing heavily in new technology and hiring thousands more people to tackle the problem of inauthenticity on the platform. Fake accounts are often associated with false news, so this is an area that will have a huge impact on curbing the spread of inaccurate information.

- **Finding industry solutions.** All of us—from tech companies and media companies to newsrooms and classrooms—must work together to find industry solutions to strengthen the online news ecosystem and our own digital literacy. That's why we're collaborating with others who operate in this space. Last January, we announced The Facebook Journalism Project, an initiative that seeks to establish stronger ties between Facebook and the news industry. The project is focused on developing news products, providing training and tools for journalists, and working with publishers and educators on how we can equip people with the knowledge they need to be informed readers in the digital age. Since launching the Journalism Project, we've met with more than 2,600 publishers around the world to understand how they use our products and how we can make improvements to better support their needs.

- **Disrupting economic incentives.** When it comes to fighting false news, we've found that a lot of it is financially motivated. So, one of the most effective approaches is removing the economic incentives for those who traffic in inaccurate information. We've done things like block ads from pages that repeatedly share false news and significantly limit the distribution of web pages that deliver low quality web experiences.

- **Building new products.** We believe it's important to amplify the good effects of social media and mitigate the bad—to contribute to the diversity of ideas, information, and view points, while strengthening our common understanding.

    - We believe giving people more context can help them decide what to trust and what to share. The third-party fact-checking program we have developed uses reports from our community, along with other signals, to send stories to accredited third-party fact checking organizations. If the fact checking organizations identify a story as fake, we will suggest related articles in News Feed to show people different points of view, including information from fact checkers. Stories that have been disputed may also appear lower in News Feed. Our own data analytics show that a false rating from one of our fact checking partners reduces future impressions on Facebook by 80 percent.

    - We're also testing Article Context as a way of giving people more information about the material they're reading on Facebook. Since we launched this test, some of the articles people see in News Feed will feature an "i" icon that allows them to access more information at the tap of a button. The information we surface is pulled from across the internet, and includes things like the publisher's Wikipedia entry, trending articles or related articles about the topic, and information about

how the article is being shared on Facebook. In some cases, if that information is unavailable, we will let people know since that can also be helpful context.

388. Was Facebook paid by affiliates or other companies in exchange for user data?

We believe that it's important to communicate with people about the information that we collect and how people can control it. As explained in our Data Policy, we collect three basic categories of data about people:

- (1) data about things people do and share (and who they connect with) on our services;
- (2) data about the devices people use to access our services; and
- (3) data we receive from partners, including the websites and apps that use our business tools.

We collect information about the people, Pages, accounts, hashtags, and groups users are connected to and how they interact with them across our Products, such as people a user communicates with the most or groups users are part of. We also collect contact information if they choose to upload, sync, or import it from a device (such as an address book or call log or SMS log history), which we use for things like helping them and others find people they may know.

The data we use to show ads to people depends on the data we have received from people. For people who are new to Facebook, we may have minimal data that we can use. For people who have used our services for longer, we likely have more data, but the amount of data will depend on the nature of that use and how they have used our controls. Any person can see each of the specific interests we maintain about them for advertising by visiting Ads Preferences, which lets people see what interests we use to choose ads for them—and to edit or delete these interests. We also provide more detailed information about how we use data to decide what ads to show to people in our "About Facebook Ads" page, at https://www.facebook.com/ads/about. And, we do not sell people's information to anyone, and we never will.

All users must expressly consent to Facebook's Terms and Data Policy when registering for Facebook. The Data Policy explains the kinds of information we collect, how we use this information, how we share this information, and how users can manage and delete information.

Facebook does not create profiles for people without a Facebook account, but we do receive some information from devices and browsers that may be used by non-users. For example:

- When people visit apps or websites that feature our technologies—like the Facebook Like or Comment button—our servers automatically log (i) standard browser or app records of the fact that a particular device or user visited the website or app (this connection to Facebook's servers occurs automatically when a person visits a website or app that contains our technologies, such as a Like button, and is an inherent function of Internet design); and (ii) any additional information the publisher of the app or website chooses to share with Facebook about the person's activities on that site (such as the fact that a

purchase was made on the site). This is a standard feature of the Internet, and most websites and apps share this same information with multiple different third-parties whenever people visit their website or app. When the person visiting a website featuring Facebook's tools is not a registered Facebook user, Facebook does not have information identifying that individual, and it does not create profiles for this individual.

- We also may receive information about the device of a non-registered user if that user visits a part of Facebook that does not require people to log in—such as a public Facebook Page. The information we log when people visit our websites or apps is the same as described above and is the same information that any provider of an online service would receive.

- In addition, Facebook may receive some basic information about devices where Facebook apps are installed, including before people using those devices have registered for Facebook (such as when a user downloads a Facebook app, but has not yet created an account, or if the app is preloaded on a given device). This device data includes things like device model, operating system, IP address, app version and device identifiers. We use this information to provide the right version of the app, help people who want to create accounts (for example, optimizing the registration flow for the specific device), retrieving bug fixes and measuring and improving app performance. We do not use this information to build profiles about non-registered users.

389. How does keeping users' information private benefit Facebook?

We believe that it's important to communicate with people about the information that we collect and how people can control it. As explained in our Data Policy, we collect three basic categories of data about people:

- (1) data about things people do and share (and who they connect with) on our services;

- (2) data about the devices people use to access our services; and

- (3) data we receive from partners, including the websites and apps that use our business tools.

We collect information about the people, Pages, accounts, hashtags, and groups users are connected to and how they interact with them across our Products, such as people a user communicates with the most or groups users are part of. We also collect contact information if they choose to upload, sync, or import it from a device (such as an address book or call log or SMS log history), which we use for things like helping them and others find people they may know.

The data we use to show ads to people depends on the data we have received from people. For people who are new to Facebook, we may have minimal data that we can use. For people who have used our services for longer, we likely have more data, but the amount of data will depend on the nature of that use and how they have used our controls. Any person can see each of the specific interests we maintain about them for advertising by visiting Ads Preferences,

which lets people see what interests we use to choose ads for them—and to edit or delete these interests. We also provide more detailed information about how we use data to decide what ads to show to people in our "About Facebook Ads" page, at https://www.facebook.com/ads/about. And, we do not sell people's information to anyone, and we never will.

All users must expressly consent to Facebook's Terms and Data Policy when registering for Facebook. The Data Policy explains the kinds of information we collect, how we use this information, how we share this information, and how users can manage and delete information.

Facebook does not create profiles for people without a Facebook account, but we do receive some information from devices and browsers that may be used by non-users. For example:

- When people visit apps or websites that feature our technologies—like the Facebook Like or Comment button—our servers automatically log (i) standard browser or app records of the fact that a particular device or user visited the website or app (this connection to Facebook's servers occurs automatically when a person visits a website or app that contains our technologies, such as a Like button, and is an inherent function of Internet design); and (ii) any additional information the publisher of the app or website chooses to share with Facebook about the person's activities on that site (such as the fact that a purchase was made on the site). This is a standard feature of the Internet, and most websites and apps share this same information with multiple different third-parties whenever people visit their website or app. When the person visiting a website featuring Facebook's tools is not a registered Facebook user, Facebook does not have information identifying that individual, and it does not create profiles for this individual.

- We also may receive information about the device of a non-registered user if that user visits a part of Facebook that does not require people to log in—such as a public Facebook Page. The information we log when people visit our websites or apps is the same as described above and is the same information that any provider of an online service would receive.

- In addition, Facebook may receive some basic information about devices where Facebook apps are installed, including before people using those devices have registered for Facebook (such as when a user downloads a Facebook app, but has not yet created an account, or if the app is preloaded on a given device). This device data includes things like device model, operating system, IP address, app version and device identifiers. We use this information to provide the right version of the app, help people who want to create accounts (for example, optimizing the registration flow for the specific device), retrieving bug fixes and measuring and improving app performance. We do not use this information to build profiles about non-registered users.

390. Why should the public trust Facebook going forward?

We believe everyone deserves good privacy controls. A user owns the information they share on Facebook. This means they decide what they share and who they share it with on Facebook, and they can change their mind. We require websites and apps who use our tools to

tell users they're collecting and sharing their information with us, and to get users' permission to do so.

Everyone has the right to expect strong protections for their information. We also need to do our part to help keep our community safe, in a way that's consistent with people's privacy expectations. We've recently announced several steps to give people more control over their privacy, including a new Privacy Shortcuts tool that we're rolling out now to give people information about how to control their information, including choosing who can see what they post and adding protections like two-factor authentication to their account. People can learn more about how to protect their privacy in our updated Data Policy and in our Privacy Basics feature (https://www.facebook.com/about/basics).

We are in the process of investigating every app that had access to a large amount of information before we changed our Platform in 2014. The investigation process is in full swing. We have large teams of internal and external experts working hard to investigate these apps as quickly as possible. As of early June 2018, thousands of apps have been investigated and around 200 apps have been suspended—pending a thorough investigation into whether they did in fact misuse any data. Where we find evidence that these or other apps did misuse data, we will ban them and let people know.

Facebook is generally not opposed to regulation but wants to ensure it is the right regulation. The issues facing the industry are complex, multi-faceted, and affect an important part of peoples' lives. As such, Facebook is absolutely committed to working with regulators, like Congress, to craft the right regulations. Facebook would be happy to review any proposed legislation and provide comments.

391. How can we be confident that FB will protect users data with business model focused on advertisers?

To build a secure product with extensive infrastructure that connects people wherever they live or whatever their income level, we need to make sure everyone can afford it. Advertising lets us keep Facebook free, which ensures it remains affordable for everyone. We also believe the ads you see across the Facebook family of apps and services should be useful and relevant to you. Users can't opt out of seeing ads altogether because selling ads is what keeps Facebook free, but they do have different options to control how their data can and can't be used to show them ads. They're all found in ad preferences, which allows users to turn off the use of all data collected from partners off Facebook to target ads. Users can also decide which of their profile fields they want used for ad targeting in the Information section under "About you." Users can remove themselves from interests under "Your interests" and categories under "Your categories." And, we do not sell people's information to anyone, and we never will.

Facebook is committed to transparency for all ads, including ads with political content. Facebook believes that people should be able to easily understand why they are seeing ads, who paid for them, and what other ads those advertisers are running. As such, Facebook only allows authorized advertisers to run ads about elections or issues that are being debated across the country. In order to be authorized by Facebook, advertisers will need to confirm their identity and location. Furthermore, all political and issue ads will include a disclosure which reads: "Paid

for by," and when users click on this disclosure they will be able to see details about the advertiser. Users will also be able to see an explanation of why they saw the particular ad. This is similar to the disclosure included on political TV advertisements. We just launched globally View Active Ads, a feature that will enable anyone to see all of the ads an advertiser is currently running by visiting the advertiser's Facebook Page.

392. What can you do (and what is being done) to assure true identities of users?

We want Facebook to be a place where people can discover more news, information, and perspectives, and we are working to build products that help to that. Through our News Feed algorithm, we also work hard to actively reduce the distribution of clickbait, sensationalism, and misinformation, on the one hand, and to boost news and information from sources that are trusted, informative, and local, on the other hand.

We are focusing on four different strategies to address misinformation:

- **Strengthening enforcement of our authenticity policies.** We are investing heavily in new technology and hiring thousands more people to tackle the problem of inauthenticity on the platform. Fake accounts are often associated with false news, so this is an area that will have a huge impact on curbing the spread of inaccurate information.

- **Finding industry solutions.** All of us—from tech companies and media companies to newsrooms and classrooms—must work together to find industry solutions to strengthen the online news ecosystem and our own digital literacy. That's why we're collaborating with others who operate in this space. Last January, we announced The Facebook Journalism Project, an initiative that seeks to establish stronger ties between Facebook and the news industry. The project is focused on developing news products, providing training and tools for journalists, and working with publishers and educators on how we can equip people with the knowledge they need to be informed readers in the digital age. Since launching the Journalism Project, we've met with more than 2,600 publishers around the world to understand how they use our products and how we can make improvements to better support their needs.

- **Disrupting economic incentives.** When it comes to fighting false news, we've found that a lot of it is financially motivated. So, one of the most effective approaches is removing the economic incentives for those who traffic in inaccurate information. We've done things like block ads from pages that repeatedly share false news and significantly limit the distribution of web pages that deliver low quality web experiences.

- **Building new products.** We believe it's important to amplify the good effects of social media and mitigate the bad—to contribute to the diversity of ideas, information, and view points, while strengthening our common understanding.

    - We believe giving people more context can help them decide what to trust and what to share. The third-party fact-checking program we have developed uses reports from our community, along with other signals, to send stories to accredited third-party fact checking organizations. If the fact checking organizations identify a story as fake, we will suggest related articles in News

Feed to show people different points of view, including information from fact checkers. Stories that have been disputed may also appear lower in News Feed. Our own data analytics show that a false rating from one of our fact checking partners reduces future impressions on Facebook by 80 percent.

- We're also testing Article Context as a way of giving people more information about the material they're reading on Facebook. Since we launched this test, some of the articles people see in News Feed will feature an "i" icon that allows them to access more information at the tap of a button. The information we surface is pulled from across the internet, and includes things like the publisher's Wikipedia entry, trending articles or related articles about the topic, and information about how the article is being shared on Facebook. In some cases, if that information is unavailable, we will let people know since that can also be helpful context.

393. What does Facebook sell and to whom?

We believe that it's important to communicate with people about the information that we collect and how people can control it. As explained in our Data Policy, we collect three basic categories of data about people:

- (1) data about things people do and share (and who they connect with) on our services;
- (2) data about the devices people use to access our services; and
- (3) data we receive from partners, including the websites and apps that use our business tools.

We collect information about the people, Pages, accounts, hashtags, and groups users are connected to and how they interact with them across our Products, such as people a user communicates with the most or groups users are part of. We also collect contact information if they choose to upload, sync, or import it from a device (such as an address book or call log or SMS log history), which we use for things like helping them and others find people they may know.

The data we use to show ads to people depends on the data we have received from people. For people who are new to Facebook, we may have minimal data that we can use. For people who have used our services for longer, we likely have more data, but the amount of data will depend on the nature of that use and how they have used our controls. Any person can see each of the specific interests we maintain about them for advertising by visiting Ads Preferences, which lets people see what interests we use to choose ads for them—and to edit or delete these interests. We also provide more detailed information about how we use data to decide what ads to show to people in our "About Facebook Ads" page, at https://www.facebook.com/ads/about. And, we do not sell people's information to anyone, and we never will.

All users must expressly consent to Facebook's Terms and Data Policy when registering for Facebook. The Data Policy explains the kinds of information we collect, how we use this information, how we share this information, and how users can manage and delete information.

Facebook does not create profiles for people without a Facebook account, but we do receive some information from devices and browsers that may be used by non-users. For example:

- When people visit apps or websites that feature our technologies—like the Facebook Like or Comment button—our servers automatically log (i) standard browser or app records of the fact that a particular device or user visited the website or app (this connection to Facebook's servers occurs automatically when a person visits a website or app that contains our technologies, such as a Like button, and is an inherent function of Internet design); and (ii) any additional information the publisher of the app or website chooses to share with Facebook about the person's activities on that site (such as the fact that a purchase was made on the site). This is a standard feature of the Internet, and most websites and apps share this same information with multiple different third-parties whenever people visit their website or app. When the person visiting a website featuring Facebook's tools is not a registered Facebook user, Facebook does not have information identifying that individual, and it does not create profiles for this individual.

- We also may receive information about the device of a non-registered user if that user visits a part of Facebook that does not require people to log in—such as a public Facebook Page. The information we log when people visit our websites or apps is the same as described above and is the same information that any provider of an online service would receive.

- In addition, Facebook may receive some basic information about devices where Facebook apps are installed, including before people using those devices have registered for Facebook (such as when a user downloads a Facebook app, but has not yet created an account, or if the app is preloaded on a given device). This device data includes things like device model, operating system, IP address, app version and device identifiers. We use this information to provide the right version of the app, help people who want to create accounts (for example, optimizing the registration flow for the specific device), retrieving bug fixes and measuring and improving app performance. We do not use this information to build profiles about non-registered users.

394. Have your original intentions, priorities and goals changed, and if so, why. And how?

We believe everyone deserves good privacy controls. A user owns the information they share on Facebook. This means they decide what they share and who they share it with on Facebook, and they can change their mind. We require websites and apps who use our tools to tell users they're collecting and sharing their information with us, and to get users' permission to do so.

Everyone has the right to expect strong protections for their information. We also need to do our part to help keep our community safe, in a way that's consistent with people's privacy expectations. We've recently announced several steps to give people more control over their privacy, including a new Privacy Shortcuts tool that we're rolling out now to give people information about how to control their information, including choosing who can see what they

post and adding protections like two-factor authentication to their account. People can learn more about how to protect their privacy in our updated Data Policy and in our Privacy Basics feature (https://www.facebook.com/about/basics).

We are in the process of investigating every app that had access to a large amount of information before we changed our Platform in 2014. The investigation process is in full swing. We have large teams of internal and external experts working hard to investigate these apps as quickly as possible. As of early June 2018, thousands of apps have been investigated and around 200 apps have been suspended—pending a thorough investigation into whether they did in fact misuse any data. Where we find evidence that these or other apps did misuse data, we will ban them and let people know.

Facebook is generally not opposed to regulation but wants to ensure it is the right regulation. The issues facing the industry are complex, multi-faceted, and affect an important part of peoples' lives. As such, Facebook is absolutely committed to working with regulators, like Congress, to craft the right regulations. Facebook would be happy to review any proposed legislation and provide comments.

395. What percent of your revenue is from sharing user data with third parties?

We believe that it's important to communicate with people about the information that we collect and how people can control it. As explained in our Data Policy, we collect three basic categories of data about people:

- (1) data about things people do and share (and who they connect with) on our services;
- (2) data about the devices people use to access our services; and
- (3) data we receive from partners, including the websites and apps that use our business tools.

We collect information about the people, Pages, accounts, hashtags, and groups users are connected to and how they interact with them across our Products, such as people a user communicates with the most or groups users are part of. We also collect contact information if they choose to upload, sync, or import it from a device (such as an address book or call log or SMS log history), which we use for things like helping them and others find people they may know.

The data we use to show ads to people depends on the data we have received from people. For people who are new to Facebook, we may have minimal data that we can use. For people who have used our services for longer, we likely have more data, but the amount of data will depend on the nature of that use and how they have used our controls. Any person can see each of the specific interests we maintain about them for advertising by visiting Ads Preferences, which lets people see what interests we use to choose ads for them—and to edit or delete these interests. We also provide more detailed information about how we use data to decide what ads to show to people in our "About Facebook Ads" page, at https://www.facebook.com/ads/about. And, we do not sell people's information to anyone, and we never will.

All users must expressly consent to Facebook's Terms and Data Policy when registering for Facebook. The Data Policy explains the kinds of information we collect, how we use this information, how we share this information, and how users can manage and delete information.

Facebook does not create profiles for people without a Facebook account, but we do receive some information from devices and browsers that may be used by non-users. For example:

- When people visit apps or websites that feature our technologies—like the Facebook Like or Comment button—our servers automatically log (i) standard browser or app records of the fact that a particular device or user visited the website or app (this connection to Facebook's servers occurs automatically when a person visits a website or app that contains our technologies, such as a Like button, and is an inherent function of Internet design); and (ii) any additional information the publisher of the app or website chooses to share with Facebook about the person's activities on that site (such as the fact that a purchase was made on the site). This is a standard feature of the Internet, and most websites and apps share this same information with multiple different third-parties whenever people visit their website or app. When the person visiting a website featuring Facebook's tools is not a registered Facebook user, Facebook does not have information identifying that individual, and it does not create profiles for this individual.

- We also may receive information about the device of a non-registered user if that user visits a part of Facebook that does not require people to log in—such as a public Facebook Page. The information we log when people visit our websites or apps is the same as described above and is the same information that any provider of an online service would receive.

- In addition, Facebook may receive some basic information about devices where Facebook apps are installed, including before people using those devices have registered for Facebook (such as when a user downloads a Facebook app, but has not yet created an account, or if the app is preloaded on a given device). This device data includes things like device model, operating system, IP address, app version and device identifiers. We use this information to provide the right version of the app, help people who want to create accounts (for example, optimizing the registration flow for the specific device), retrieving bug fixes and measuring and improving app performance. We do not use this information to build profiles about non-registered users.

396. Is Facebook collecting data on citizens for the purpose of monitoring people to increase profits?

We believe that it's important to communicate with people about the information that we collect and how people can control it. As explained in our Data Policy, we collect three basic categories of data about people:

(1) data about things people do and share (and who they connect with) on our services;

(2) data about the devices people use to access our services; and

(3) data we receive from partners, including the websites and apps that use our business tools.

We collect information about the people, Pages, accounts, hashtags, and groups users are connected to and how they interact with them across our Products, such as people a user communicates with the most or groups users are part of. We also collect contact information if they choose to upload, sync, or import it from a device (such as an address book or call log or SMS log history), which we use for things like helping them and others find people they may know.

The data we use to show ads to people depends on the data we have received from people. For people who are new to Facebook, we may have minimal data that we can use. For people who have used our services for longer, we likely have more data, but the amount of data will depend on the nature of that use and how they have used our controls. Any person can see each of the specific interests we maintain about them for advertising by visiting Ads Preferences, which lets people see what interests we use to choose ads for them—and to edit or delete these interests. We also provide more detailed information about how we use data to decide what ads to show to people in our "About Facebook Ads" page, at https://www.facebook.com/ads/about. And, we do not sell people's information to anyone, and we never will.

All users must expressly consent to Facebook's Terms and Data Policy when registering for Facebook. The Data Policy explains the kinds of information we collect, how we use this information, how we share this information, and how users can manage and delete information.

Facebook does not create profiles for people without a Facebook account, but we do receive some information from devices and browsers that may be used by non-users. For example:

- When people visit apps or websites that feature our technologies—like the Facebook Like or Comment button—our servers automatically log (i) standard browser or app records of the fact that a particular device or user visited the website or app (this connection to Facebook's servers occurs automatically when a person visits a website or app that contains our technologies, such as a Like button, and is an inherent function of Internet design); and (ii) any additional information the publisher of the app or website chooses to share with Facebook about the person's activities on that site (such as the fact that a purchase was made on the site). This is a standard feature of the Internet, and most websites and apps share this same information with multiple different third-parties whenever people visit their website or app. When the person visiting a website featuring Facebook's tools is not a registered Facebook user, Facebook does not have information identifying that individual, and it does not create profiles for this individual.

- We also may receive information about the device of a non-registered user if that user visits a part of Facebook that does not require people to log in—such as a public Facebook Page. The information we log when people visit our websites or apps is the same as described above and is the same information that any provider of an online service would receive.

- In addition, Facebook may receive some basic information about devices where Facebook apps are installed, including before people using those devices have registered for Facebook (such as when a user downloads a Facebook app, but has not yet created an account, or if the app is preloaded on a given device). This device data includes things like device model, operating system, IP address, app version and device identifiers. We use this information to provide the right version of the app, help people who want to create accounts (for example, optimizing the registration flow for the specific device), retrieving bug fixes and measuring and improving app performance. We do not use this information to build profiles about non-registered users.

397. Why should Facebook users need to pay you for full data privacy?

We believe that it's important to communicate with people about the information that we collect and how people can control it. As explained in our Data Policy, we collect three basic categories of data about people:

(1) data about things people do and share (and who they connect with) on our services;

(2) data about the devices people use to access our services; and

(3) data we receive from partners, including the websites and apps that use our business tools.

We collect information about the people, Pages, accounts, hashtags, and groups users are connected to and how they interact with them across our Products, such as people a user communicates with the most or groups users are part of. We also collect contact information if they choose to upload, sync, or import it from a device (such as an address book or call log or SMS log history), which we use for things like helping them and others find people they may know.

The data we use to show ads to people depends on the data we have received from people. For people who are new to Facebook, we may have minimal data that we can use. For people who have used our services for longer, we likely have more data, but the amount of data will depend on the nature of that use and how they have used our controls. Any person can see each of the specific interests we maintain about them for advertising by visiting Ads Preferences, which lets people see what interests we use to choose ads for them—and to edit or delete these interests. We also provide more detailed information about how we use data to decide what ads to show to people in our "About Facebook Ads" page, at https://www.facebook.com/ads/about. And, we do not sell people's information to anyone, and we never will.

All users must expressly consent to Facebook's Terms and Data Policy when registering for Facebook. The Data Policy explains the kinds of information we collect, how we use this information, how we share this information, and how users can manage and delete information.

Facebook does not create profiles for people without a Facebook account, but we do receive some information from devices and browsers that may be used by non-users. For example:

- When people visit apps or websites that feature our technologies—like the Facebook Like or Comment button—our servers automatically log (i) standard browser or app records of the fact that a particular device or user visited the website or app (this connection to Facebook's servers occurs automatically when a person visits a website or app that contains our technologies, such as a Like button, and is an inherent function of Internet design); and (ii) any additional information the publisher of the app or website chooses to share with Facebook about the person's activities on that site (such as the fact that a purchase was made on the site). This is a standard feature of the Internet, and most websites and apps share this same information with multiple different third-parties whenever people visit their website or app. When the person visiting a website featuring Facebook's tools is not a registered Facebook user, Facebook does not have information identifying that individual, and it does not create profiles for this individual.

- We also may receive information about the device of a non-registered user if that user visits a part of Facebook that does not require people to log in—such as a public Facebook Page. The information we log when people visit our websites or apps is the same as described above and is the same information that any provider of an online service would receive.

- In addition, Facebook may receive some basic information about devices where Facebook apps are installed, including before people using those devices have registered for Facebook (such as when a user downloads a Facebook app, but has not yet created an account, or if the app is preloaded on a given device). This device data includes things like device model, operating system, IP address, app version and device identifiers. We use this information to provide the right version of the app, help people who want to create accounts (for example, optimizing the registration flow for the specific device), retrieving bug fixes and measuring and improving app performance. We do not use this information to build profiles about non-registered users.

398. Isn't Facebook's Board complicit after years of transgressions and apologies by management?

We recognize that we have made mistakes, and we are committed to learning from this experience to secure our platform further and make our community safer for everyone going forward. As our CEO Mark Zuckerberg has said, when you are building something unprecedented like Facebook, there are going to be mistakes. What people should hold us accountable for is learning from the mistakes and continually doing better—and, at the end of the day, making sure that we're building things that people like and that make their lives better.

Particularly in the past few months, we've realized that we need to take a broader view of our responsibility to our community. Part of that effort is continuing our ongoing efforts to identify ways that we can improve our privacy practices. We've heard loud and clear that privacy settings and other important tools are too hard to find and that we must do more to keep people informed. So, we're taking additional steps to put people more in control of their privacy. For instance, we redesigned our entire settings menu on mobile devices from top to bottom to make things easier to find. We also created a new Privacy Shortcuts in a menu where users can control their data in just a few taps, with clearer explanations of how our controls work. The experience

is now clearer, more visual, and easy-to-find. Furthermore, we also updated our terms of service that include our commitments to everyone using Facebook. We explain the services we offer in language that's easier to read. We've also updated our Data Policy to better spell out what data we collect and how we use it in Facebook, Instagram, Messenger, and other products.

399. If individual Facebook employees were using Facebook's internal data & surveillance tools to commit crimes or violate the law, would Facebook have any way of knowing this was occurring?

Protecting people's data is one of our most important responsibilities, and we are committed to continuing our work to improve how we protect people's information and to working with regulators to draft appropriate regulations. Our mission is to give people the power to build community and bring the world closer together. As the internet becomes more important in people's lives, the real question is about the right set of regulations that should apply to all internet services, regardless of size. Across the board, we have a responsibility to not just build tools, but to make sure that they're used in ways that are positive for our users. Facebook is generally not opposed to regulation but wants to ensure it is the right regulation. The issues facing the industry are complex, multi-faceted, and affect an important part of peoples' lives. As such, Facebook is absolutely committed to working with regulators, like Congress, to craft the right regulations.

We are already regulated in many ways—for example, under the Federal Trade Commission Act—and we are subject to ongoing oversight by the FTC under the terms of a 2011 consent order. We furnished extensive information to the FTC regarding the ability for users to port their Facebook data (including friends data that had been shared with them) with apps on Facebook's platform, as part of the FTC's investigation culminating in the July 27, 2012 Consent Order. The Consent Order memorializes the agreement between Facebook and the FTC and did not require Facebook to turn off or change the ability for people to port friends data that had been shared with them on Facebook to apps they used. Facebook voluntarily changed this feature of Platform in 2014, however. Facebook has not violated the Federal Trade Commission Act. Facebook is not in a position to determine whether third-party app developers violated the Act and leaves that determination to the FTC, although we can confirm that misrepresenting the terms of an app to users is a violation of Facebook's developer policies.

Facebook has inherent incentives to protect its customers' privacy and address breaches and vulnerabilities. Indeed, the recent discovery of misconduct by an app developer on the Facebook platform clearly hurt Facebook and made it harder for us to achieve our social mission. As such, Facebook is committed to protecting our platform from bad actors, ensuring we are able to continue our mission of giving people a voice and bringing them closer together. It will take some time to work through all the changes we need to make across the company, but Facebook is committed to getting this right.

400. Did Facebook ever consider that selling personal information would be used for political targeting?

We want our platform to be a place where people can have authentic conversations about elections and other political topics. We believe this kind of engagement promotes democracy,

but we know that there are actors working to interfere with those conversations and undermine our elections. We are already taking steps to proactively prevent election interference and we are strengthening these protections going forward.

Engagement with campaigns: We want all candidates, groups, and voters to use our platform to engage in elections. We want it to be easy for people to find, follow, and contact their elected representatives—and those running to represent them. That's why, for candidates across the political spectrum, Facebook offers the same levels of support in key moments to help campaigns understand how best to use the platform. Both the Obama and Romney campaigns had access to the same tools, and no campaign received any special treatment from Facebook. Likewise, we offered identical support to both the Trump and Clinton campaigns, and had teams assigned to both. Everyone had access to the same tools, which are the same tools that every campaign is offered, and is consistent with support provided to commercial clients in the normal course of business. Facebook representatives advise political advertisers on Facebook, as they would with other, non-political managed accounts. We have a compliance team that trains our sales representatives to comply with all federal election law requirements in this area.

While no one from Facebook was assigned full-time to the Trump campaign, Facebook employees did interact with Cambridge Analytica employees. While our investigation is ongoing, our review indicates that Facebook employees did not identify any issues involving the improper use of Facebook data in the course of their interactions with Cambridge Analytica during the 2016 US Presidential campaign.

Election Integrity: In the run-up to the 2016 elections, we were focused on the kinds of cybersecurity attacks typically used by nation states, for example phishing and malware attacks. And we were too slow to spot information operations interference. Since then, we've made important changes to prevent bad actors from using misinformation to undermine the democratic process. This will never be a solved problem because we're up against determined, creative and well-funded adversaries. But we are making steady progress. Here is a list of the 10 most important changes we have made:

- **Ads transparency.** Advertising should be transparent: users should be able to see all the ads an advertiser is currently running on Facebook, Instagram and Messenger. And for ads with political content, we've created an archive that will hold ads with political content for seven years—including information about ad impressions and spend, as well as demographic data such as age, gender and location. People in Canada and Ireland have already been able to see all the ads that a Page is running on Facebook—and we've launched this globally.

- **Verification and labeling.** Every advertiser will now need to confirm their ID and location before being able to run any ads with political content in the US. All ads with political content will also clearly state who paid for them.

- **Updating targeting.** We want ads on Facebook to be safe and civil. We thoroughly review the targeting criteria advertisers can use to ensure they are consistent with our principles. As a result, we removed nearly one-third of the targeting segments used by the IRA. We continue to allow some criteria that people may find controversial. But we do

see businesses marketing things like historical books, documentaries or television shows using them in legitimate ways.

- **Better technology.** Over the past year, we've gotten increasingly better at finding and disabling fake accounts. We now block millions of fake accounts each day as people try to create them—and before they've done any harm. This is thanks to improvements in machine learning and artificial intelligence, which can proactively identify suspicious behavior at a scale that was not possible before—without needing to look at the content itself.

- **Action to tackle fake news.** We are working hard to stop the spread of false news. We work with third-party fact-checking organizations to limit the spread of articles rated false. To reduce the spread of false news, we remove fake accounts and disrupt economic incentives for traffickers of misinformation. We also use various signals, including feedback from our community, to identify potential false news. In countries where we have partnerships with independent third-party fact-checkers, stories rated as false by those fact-checkers are shown lower in News Feed. If Pages or domains repeatedly create or share misinformation, we significantly reduce their distribution and remove their advertising rights. We also want to empower people to decide for themselves what to read, trust, and share. We promote news literacy and work to inform people with more context. For example, if third-party fact-checkers write articles about a news story, we show them immediately below the story in the Related Articles unit. We also notify people and Page Admins if they try to share a story, or have shared one in the past, that's been determined to be false. In addition to our own efforts, we're learning from academics, scaling our partnerships with third-party fact-checkers and talking to other organizations about how we can work together.

  A key focus is working to disrupt the economics of fake news. For example, preventing the creation of fake accounts that spread it, banning sites that engage in this behavior from using our ad products, and demoting articles found to be false by fact checkers in News Feed—causing it to lose 80% of its traffic. We now work with independent fact checkers in the US, France, Germany, Ireland, the Netherlands, Italy, Mexico, Colombia, India, Indonesia and the Philippines with plans to scale to more countries in the coming months.

- **Significant investments in security.** We're doubling the number of people working on safety and security from 10,000 last year to over 20,000 this year. We expect these investments to impact our profitability. But the safety of people using Facebook needs to come before profit.

- **Industry collaboration.** Recently, we joined 34 global tech and security companies in signing a TechAccord pact to help improve security for everyone.

- **Information sharing and reporting channels.** In the 2017 German elections, we worked closely with the authorities there, including the Federal Office for Information Security (BSI). This gave them a dedicated reporting channel for security issues related to the federal elections.

- **Tracking 40+ elections.** In recent months, we've started to deploy new tools and teams to proactively identify threats in the run-up to specific elections. We first tested this effort during the Alabama Senate election, and plan to continue these efforts for elections around the globe, including the US midterms. Last year we used public service announcements to help inform people about fake news in 21 separate countries, including in advance of French, Kenyan and German elections.

- **Action against the Russia-based IRA.** In April, we removed 70 Facebook and 65 Instagram accounts—as well as 138 Facebook Pages—controlled by the IRA primarily targeted either at people living in Russia or Russian-speakers around the world including from neighboring countries like Azerbaijan, Uzbekistan and Ukraine. The IRA has repeatedly used complex networks of inauthentic accounts to deceive and manipulate people in the US, Europe and Russia—and we don't want them on Facebook anywhere in the world.

401. Does FB consider users as stakeholders or as ones to deceive?

We believe that it's important to communicate with people about the information that we collect and how people can control it. As explained in our Data Policy, we collect three basic categories of data about people:

(1) data about things people do and share (and who they connect with) on our services;

(2) data about the devices people use to access our services; and

(3) data we receive from partners, including the websites and apps that use our business tools.

We collect information about the people, Pages, accounts, hashtags, and groups users are connected to and how they interact with them across our Products, such as people a user communicates with the most or groups users are part of. We also collect contact information if they choose to upload, sync, or import it from a device (such as an address book or call log or SMS log history), which we use for things like helping them and others find people they may know.

The data we use to show ads to people depends on the data we have received from people. For people who are new to Facebook, we may have minimal data that we can use. For people who have used our services for longer, we likely have more data, but the amount of data will depend on the nature of that use and how they have used our controls. Any person can see each of the specific interests we maintain about them for advertising by visiting Ads Preferences, which lets people see what interests we use to choose ads for them—and to edit or delete these interests. We also provide more detailed information about how we use data to decide what ads to show to people in our "About Facebook Ads" page, at https://www.facebook.com/ads/about. And, we do not sell people's information to anyone, and we never will.

All users must expressly consent to Facebook's Terms and Data Policy when registering for Facebook. The Data Policy explains the kinds of information we collect, how we use this information, how we share this information, and how users can manage and delete information.

Facebook does not create profiles for people without a Facebook account, but we do receive some information from devices and browsers that may be used by non-users. For example:

- When people visit apps or websites that feature our technologies—like the Facebook Like or Comment button—our servers automatically log (i) standard browser or app records of the fact that a particular device or user visited the website or app (this connection to Facebook's servers occurs automatically when a person visits a website or app that contains our technologies, such as a Like button, and is an inherent function of Internet design); and (ii) any additional information the publisher of the app or website chooses to share with Facebook about the person's activities on that site (such as the fact that a purchase was made on the site). This is a standard feature of the Internet, and most websites and apps share this same information with multiple different third-parties whenever people visit their website or app. When the person visiting a website featuring Facebook's tools is not a registered Facebook user, Facebook does not have information identifying that individual, and it does not create profiles for this individual.

- We also may receive information about the device of a non-registered user if that user visits a part of Facebook that does not require people to log in—such as a public Facebook Page. The information we log when people visit our websites or apps is the same as described above and is the same information that any provider of an online service would receive.

- In addition, Facebook may receive some basic information about devices where Facebook apps are installed, including before people using those devices have registered for Facebook (such as when a user downloads a Facebook app, but has not yet created an account, or if the app is preloaded on a given device). This device data includes things like device model, operating system, IP address, app version and device identifiers. We use this information to provide the right version of the app, help people who want to create accounts (for example, optimizing the registration flow for the specific device), retrieving bug fixes and measuring and improving app performance. We do not use this information to build profiles about non-registered users.

402. FBs revenue model relies on selling personal info. Could a paid model satisfy your investors? And bring in enough revenue for FB to survive?

We believe that it's important to communicate with people about the information that we collect and how people can control it. As explained in our Data Policy, we collect three basic categories of data about people:

(1) data about things people do and share (and who they connect with) on our services;

(2) data about the devices people use to access our services; and

(3) data we receive from partners, including the websites and apps that use our business tools.

We collect information about the people, Pages, accounts, hashtags, and groups users are connected to and how they interact with them across our Products, such as people a user communicates with the most or groups users are part of. We also collect contact information if they choose to upload, sync, or import it from a device (such as an address book or call log or SMS log history), which we use for things like helping them and others find people they may know.

The data we use to show ads to people depends on the data we have received from people. For people who are new to Facebook, we may have minimal data that we can use. For people who have used our services for longer, we likely have more data, but the amount of data will depend on the nature of that use and how they have used our controls. Any person can see each of the specific interests we maintain about them for advertising by visiting Ads Preferences, which lets people see what interests we use to choose ads for them—and to edit or delete these interests. We also provide more detailed information about how we use data to decide what ads to show to people in our "About Facebook Ads" page, at https://www.facebook.com/ads/about. And, we do not sell people's information to anyone, and we never will.

All users must expressly consent to Facebook's Terms and Data Policy when registering for Facebook. The Data Policy explains the kinds of information we collect, how we use this information, how we share this information, and how users can manage and delete information.

Facebook does not create profiles for people without a Facebook account, but we do receive some information from devices and browsers that may be used by non-users. For example:

- When people visit apps or websites that feature our technologies—like the Facebook Like or Comment button—our servers automatically log (i) standard browser or app records of the fact that a particular device or user visited the website or app (this connection to Facebook's servers occurs automatically when a person visits a website or app that contains our technologies, such as a Like button, and is an inherent function of Internet design); and (ii) any additional information the publisher of the app or website chooses to share with Facebook about the person's activities on that site (such as the fact that a purchase was made on the site). This is a standard feature of the Internet, and most websites and apps share this same information with multiple different third-parties whenever people visit their website or app. When the person visiting a website featuring Facebook's tools is not a registered Facebook user, Facebook does not have information identifying that individual, and it does not create profiles for this individual.

- We also may receive information about the device of a non-registered user if that user visits a part of Facebook that does not require people to log in—such as a public Facebook Page. The information we log when people visit our websites or apps is the same as described above and is the same information that any provider of an online service would receive.

- In addition, Facebook may receive some basic information about devices where Facebook apps are installed, including before people using those devices have registered for Facebook (such as when a user downloads a Facebook app, but has not yet created an

account, or if the app is preloaded on a given device). This device data includes things like device model, operating system, IP address, app version and device identifiers. We use this information to provide the right version of the app, help people who want to create accounts (for example, optimizing the registration flow for the specific device), retrieving bug fixes and measuring and improving app performance. We do not use this information to build profiles about non-registered users.

403. Why is Facebook deleting accounts of Palestinians at the request of the Israeli govt? This is unfair political censorship and a double standard!

Freedom of expression is one of our core values, and we believe that adding voices to the conversation creates a richer and more vibrant community. We want people to feel confident that our community welcomes all viewpoints and we are committed to designing our products to give all people a voice and foster the free flow of ideas and culture. We recognize how important it is for Facebook to be a place where people feel empowered to communicate, and we take our role in keeping abuse off our service seriously. Our mission entails embracing diverse views. We err on the side of allowing content, even when some find it objectionable, unless removing that content prevents a specific harm.

However, we are, first and foremost, a technology company. Facebook does not create or edit the content that our users post on our platform. While we seek to be a platform for a broad range of ideas, we do moderate content in good faith according to published community standards in order to keep users on the platform safe, reduce objectionable content and to make sure users participate on the platform responsibly.

404. Why didn't you listen to women when they were reporting doxxers and swatters before Trump-Pence?

Freedom of expression is one of our core values, and we believe that adding voices to the conversation creates a richer and more vibrant community. We want people to feel confident that our community welcomes all viewpoints and we are committed to designing our products to give all people a voice and foster the free flow of ideas and culture. We recognize how important it is for Facebook to be a place where people feel empowered to communicate, and we take our role in keeping abuse off our service seriously. Our mission entails embracing diverse views. We err on the side of allowing content, even when some find it objectionable, unless removing that content prevents a specific harm.

However, we are, first and foremost, a technology company. Facebook does not create or edit the content that our users post on our platform. While we seek to be a platform for a broad range of ideas, we do moderate content in good faith according to published community standards in order to keep users on the platform safe, reduce objectionable content and to make sure users participate on the platform responsibly.

405. How many lobbyists and lawyers does Facebook have? How much did it spend on lobbying last year?

Protecting people's data is one of our most important responsibilities, and we are committed to continuing our work to improve how we protect people's information and to

working with regulators to draft appropriate regulations. Our mission is to give people the power to build community and bring the world closer together. As the internet becomes more important in people's lives, the real question is about the right set of regulations that should apply to all internet services, regardless of size. Across the board, we have a responsibility to not just build tools, but to make sure that they're used in ways that are positive for our users. Facebook is generally not opposed to regulation but wants to ensure it is the right regulation. The issues facing the industry are complex, multi-faceted, and affect an important part of peoples' lives. As such, Facebook is absolutely committed to working with regulators, like Congress, to craft the right regulations.

We are already regulated in many ways—for example, under the Federal Trade Commission Act—and we are subject to ongoing oversight by the FTC under the terms of a 2011 consent order. We furnished extensive information to the FTC regarding the ability for users to port their Facebook data (including friends data that had been shared with them) with apps on Facebook's platform, as part of the FTC's investigation culminating in the July 27, 2012 Consent Order. The Consent Order memorializes the agreement between Facebook and the FTC and did not require Facebook to turn off or change the ability for people to port friends data that had been shared with them on Facebook to apps they used. Facebook voluntarily changed this feature of Platform in 2014, however. Facebook has not violated the Federal Trade Commission Act. Facebook is not in a position to determine whether third-party app developers violated the Act and leaves that determination to the FTC, although we can confirm that misrepresenting the terms of an app to users is a violation of Facebook's developer policies.

Facebook has inherent incentives to protect its customers' privacy and address breaches and vulnerabilities. Indeed, the recent discovery of misconduct by an app developer on the Facebook platform clearly hurt Facebook and made it harder for us to achieve our social mission. As such, Facebook is committed to protecting our platform from bad actors, ensuring we are able to continue our mission of giving people a voice and bringing them closer together. It will take some time to work through all the changes we need to make across the company, but Facebook is committed to getting this right.

406. My question may sound wacky, and it is really more of a suggestion, but I would like to ask him how Facebook can grow a 'conscience' going forward?

We believe everyone deserves good privacy controls. A user owns the information they share on Facebook. This means they decide what they share and who they share it with on Facebook, and they can change their mind. We require websites and apps who use our tools to tell users they're collecting and sharing their information with us, and to get users' permission to do so.

Everyone has the right to expect strong protections for their information. We also need to do our part to help keep our community safe, in a way that's consistent with people's privacy expectations. We've recently announced several steps to give people more control over their privacy, including a new Privacy Shortcuts tool that we're rolling out now to give people information about how to control their information, including choosing who can see what they post and adding protections like two-factor authentication to their account. People can learn more

about how to protect their privacy in our updated Data Policy and in our Privacy Basics feature (https://www.facebook.com/about/basics).

We are in the process of investigating every app that had access to a large amount of information before we changed our Platform in 2014. The investigation process is in full swing. We have large teams of internal and external experts working hard to investigate these apps as quickly as possible. As of early June 2018, thousands of apps have been investigated and around 200 apps have been suspended—pending a thorough investigation into whether they did in fact misuse any data. Where we find evidence that these or other apps did misuse data, we will ban them and let people know.

Facebook is generally not opposed to regulation but wants to ensure it is the right regulation. The issues facing the industry are complex, multi-faceted, and affect an important part of peoples' lives. As such, Facebook is absolutely committed to working with regulators, like Congress, to craft the right regulations. Facebook would be happy to review any proposed legislation and provide comments.

407. Fact: If I stole a pizza, I'd be in jail. Why shouldn't you and other Facebook execs be in jail? (that happened to a person in Palo Alto)

As discussed with your staff, this question is not germane to the hearing.

408. Recent press reports indicate that messages you have sent to others at Facebook have been "recalled," or deleted, from their inboxes. It's widely known that your company is under investigation once again by the Federal Trade Commission. Can you explain to the committee why you are deleting your messages—which many might call evidence—in the middle of a federal investigation?

Protecting people's data is one of our most important responsibilities, and we are committed to continuing our work to improve how we protect people's information and to working with regulators to draft appropriate regulations. Our mission is to give people the power to build community and bring the world closer together. As the internet becomes more important in people's lives, the real question is about the right set of regulations that should apply to all internet services, regardless of size. Across the board, we have a responsibility to not just build tools, but to make sure that they're used in ways that are positive for our users. Facebook is generally not opposed to regulation but wants to ensure it is the right regulation. The issues facing the industry are complex, multi-faceted, and affect an important part of peoples' lives. As such, Facebook is absolutely committed to working with regulators, like Congress, to craft the right regulations.

We are already regulated in many ways—for example, under the Federal Trade Commission Act—and we are subject to ongoing oversight by the FTC under the terms of a 2011 consent order. We furnished extensive information to the FTC regarding the ability for users to port their Facebook data (including friends data that had been shared with them) with apps on Facebook's platform, as part of the FTC's investigation culminating in the July 27, 2012 Consent Order. The Consent Order memorializes the agreement between Facebook and the FTC and did not require Facebook to turn off or change the ability for people to port friends data that had been

shared with them on Facebook to apps they used. Facebook voluntarily changed this feature of Platform in 2014, however. Facebook has not violated the Federal Trade Commission Act. Facebook is not in a position to determine whether third-party app developers violated the Act and leaves that determination to the FTC, although we can confirm that misrepresenting the terms of an app to users is a violation of Facebook's developer policies.

Facebook has inherent incentives to protect its customers' privacy and address breaches and vulnerabilities. Indeed, the recent discovery of misconduct by an app developer on the Facebook platform clearly hurt Facebook and made it harder for us to achieve our social mission. As such, Facebook is committed to protecting our platform from bad actors, ensuring we are able to continue our mission of giving people a voice and bringing them closer together. It will take some time to work through all the changes we need to make across the company, but Facebook is committed to getting this right.

409. Do you consider yourself a "true" American patriot? If "yes": How do you reconcile that with your company's behavior?

As discussed with your staff, this question is not germane to the hearing.

410. Do you consider the people who use FB commodities or customers?

We believe that it's important to communicate with people about the information that we collect and how people can control it. As explained in our Data Policy, we collect three basic categories of data about people:

(1) data about things people do and share (and who they connect with) on our services;

(2) data about the devices people use to access our services; and

(3) data we receive from partners, including the websites and apps that use our business tools.

We collect information about the people, Pages, accounts, hashtags, and groups users are connected to and how they interact with them across our Products, such as people a user communicates with the most or groups users are part of. We also collect contact information if they choose to upload, sync, or import it from a device (such as an address book or call log or SMS log history), which we use for things like helping them and others find people they may know.

The data we use to show ads to people depends on the data we have received from people. For people who are new to Facebook, we may have minimal data that we can use. For people who have used our services for longer, we likely have more data, but the amount of data will depend on the nature of that use and how they have used our controls. Any person can see each of the specific interests we maintain about them for advertising by visiting Ads Preferences, which lets people see what interests we use to choose ads for them—and to edit or delete these interests. We also provide more detailed information about how we use data to decide what ads to show to people in our "About Facebook Ads" page, at https://www.facebook.com/ads/about. And, we do not sell people's information to anyone, and we never will.

All users must expressly consent to Facebook's Terms and Data Policy when registering for Facebook. The Data Policy explains the kinds of information we collect, how we use this information, how we share this information, and how users can manage and delete information.

Facebook does not create profiles for people without a Facebook account, but we do receive some information from devices and browsers that may be used by non-users. For example:

- When people visit apps or websites that feature our technologies—like the Facebook Like or Comment button—our servers automatically log (i) standard browser or app records of the fact that a particular device or user visited the website or app (this connection to Facebook's servers occurs automatically when a person visits a website or app that contains our technologies, such as a Like button, and is an inherent function of Internet design); and (ii) any additional information the publisher of the app or website chooses to share with Facebook about the person's activities on that site (such as the fact that a purchase was made on the site). This is a standard feature of the Internet, and most websites and apps share this same information with multiple different third-parties whenever people visit their website or app. When the person visiting a website featuring Facebook's tools is not a registered Facebook user, Facebook does not have information identifying that individual, and it does not create profiles for this individual.

- We also may receive information about the device of a non-registered user if that user visits a part of Facebook that does not require people to log in—such as a public Facebook Page. The information we log when people visit our websites or apps is the same as described above and is the same information that any provider of an online service would receive.

- In addition, Facebook may receive some basic information about devices where Facebook apps are installed, including before people using those devices have registered for Facebook (such as when a user downloads a Facebook app, but has not yet created an account, or if the app is preloaded on a given device). This device data includes things like device model, operating system, IP address, app version and device identifiers. We use this information to provide the right version of the app, help people who want to create accounts (for example, optimizing the registration flow for the specific device), retrieving bug fixes and measuring and improving app performance. We do not use this information to build profiles about non-registered users.

411. Rather than be a force for the democratic good, Facebook is in the terrible position of supporting the rise of fascism and hatred in the US. Would Facebook be willing to start a grant program, like the one it developed for community builders, to help educate ALL American consumers about critical thinking when evaluating news, and online civility?

We want our platform to be a place where people can have authentic conversations about elections and other political topics. We believe this kind of engagement promotes democracy, but we know that there are actors working to interfere with those conversations and undermine our elections. We are already taking steps to proactively prevent election interference and we are

strengthening these protections going forward.

Engagement with campaigns: We want all candidates, groups, and voters to use our platform to engage in elections. We want it to be easy for people to find, follow, and contact their elected representatives—and those running to represent them. That's why, for candidates across the political spectrum, Facebook offers the same levels of support in key moments to help campaigns understand how best to use the platform. Both the Obama and Romney campaigns had access to the same tools, and no campaign received any special treatment from Facebook. Likewise, we offered identical support to both the Trump and Clinton campaigns, and had teams assigned to both. Everyone had access to the same tools, which are the same tools that every campaign is offered, and is consistent with support provided to commercial clients in the normal course of business. Facebook representatives advise political advertisers on Facebook, as they would with other, non-political managed accounts. We have a compliance team that trains our sales representatives to comply with all federal election law requirements in this area.

While no one from Facebook was assigned full-time to the Trump campaign, Facebook employees did interact with Cambridge Analytica employees. While our investigation is ongoing, our review indicates that Facebook employees did not identify any issues involving the improper use of Facebook data in the course of their interactions with Cambridge Analytica during the 2016 US Presidential campaign.

Election Integrity: In the run-up to the 2016 elections, we were focused on the kinds of cybersecurity attacks typically used by nation states, for example phishing and malware attacks. And we were too slow to spot information operations interference. Since then, we've made important changes to prevent bad actors from using misinformation to undermine the democratic process. This will never be a solved problem because we're up against determined, creative and well-funded adversaries. But we are making steady progress. Here is a list of the 10 most important changes we have made:

- **Ads transparency.** Advertising should be transparent: users should be able to see all the ads an advertiser is currently running on Facebook, Instagram and Messenger. And for ads with political content, we've created an archive that will hold ads with political content for seven years—including information about ad impressions and spend, as well as demographic data such as age, gender and location. People in Canada and Ireland have already been able to see all the ads that a Page is running on Facebook—and we've launched this globally.

- **Verification and labeling.** Every advertiser will now need to confirm their ID and location before being able to run any ads with political content in the US. All ads with political content will also clearly state who paid for them.

- **Updating targeting.** We want ads on Facebook to be safe and civil. We thoroughly review the targeting criteria advertisers can use to ensure they are consistent with our principles. As a result, we removed nearly one-third of the targeting segments used by the IRA. We continue to allow some criteria that people may find controversial. But we do see businesses marketing things like historical books, documentaries or television shows using them in legitimate ways.

- **Better technology.** Over the past year, we've gotten increasingly better at finding and disabling fake accounts. We now block millions of fake accounts each day as people try to create them—and before they've done any harm. This is thanks to improvements in machine learning and artificial intelligence, which can proactively identify suspicious behavior at a scale that was not possible before—without needing to look at the content itself.

- **Action to tackle fake news.** We are working hard to stop the spread of false news. We work with third-party fact-checking organizations to limit the spread of articles rated false. To reduce the spread of false news, we remove fake accounts and disrupt economic incentives for traffickers of misinformation. We also use various signals, including feedback from our community, to identify potential false news. In countries where we have partnerships with independent third-party fact-checkers, stories rated as false by those fact-checkers are shown lower in News Feed. If Pages or domains repeatedly create or share misinformation, we significantly reduce their distribution and remove their advertising rights. We also want to empower people to decide for themselves what to read, trust, and share. We promote news literacy and work to inform people with more context. For example, if third-party fact-checkers write articles about a news story, we show them immediately below the story in the Related Articles unit. We also notify people and Page Admins if they try to share a story, or have shared one in the past, that's been determined to be false. In addition to our own efforts, we're learning from academics, scaling our partnerships with third-party fact-checkers and talking to other organizations about how we can work together.

  A key focus is working to disrupt the economics of fake news. For example, preventing the creation of fake accounts that spread it, banning sites that engage in this behavior from using our ad products, and demoting articles found to be false by fact checkers in News Feed—causing it to lose 80% of its traffic. We now work with independent fact checkers in the US, France, Germany, Ireland, the Netherlands, Italy, Mexico, Colombia, India, Indonesia and the Philippines with plans to scale to more countries in the coming months.

- **Significant investments in security.** We're doubling the number of people working on safety and security from 10,000 last year to over 20,000 this year. We expect these investments to impact our profitability. But the safety of people using Facebook needs to come before profit.

- **Industry collaboration.** Recently, we joined 34 global tech and security companies in signing a TechAccord pact to help improve security for everyone.

- **Information sharing and reporting channels.** In the 2017 German elections, we worked closely with the authorities there, including the Federal Office for Information Security (BSI). This gave them a dedicated reporting channel for security issues related to the federal elections.

- **Tracking 40+ elections.** In recent months, we've started to deploy new tools and teams to proactively identify threats in the run-up to specific elections. We first tested this effort

during the Alabama Senate election, and plan to continue these efforts for elections around the globe, including the US midterms. Last year we used public service announcements to help inform people about fake news in 21 separate countries, including in advance of French, Kenyan and German elections.

- **Action against the Russia-based IRA.** In April, we removed 70 Facebook and 65 Instagram accounts—as well as 138 Facebook Pages—controlled by the IRA primarily targeted either at people living in Russia or Russian-speakers around the world including from neighboring countries like Azerbaijan, Uzbekistan and Ukraine. The IRA has repeatedly used complex networks of inauthentic accounts to deceive and manipulate people in the US, Europe and Russia—and we don't want them on Facebook anywhere in the world.

412. Facebook turned its back on all it users, for money? You should be protecting us.

As discussed with your staff, this question is not germane to the hearing.

413. How do you look at yourself in the mirror?

As discussed with your staff, this question is not germane to the hearing.

414. How could U? Does the nation, its values & its people who made U so obscenely rich mean nothing to U.

As discussed with your staff, this question is not germane to the hearing.

415. Why didn't you do anything to stop this for 2 years? You knew and did nothing!

Facebook's policies regarding third-party usage of its platform technologies have prohibited—and continue to prohibit—third-party app developers from selling or licensing user data accessed from Facebook and from sharing any user data accessed from Facebook with any ad network, data broker or other advertising or monetization-related service. We take action on potential violations of our Platform Policies based on proactive review, external reports, and other signals. Kogan was not permitted to sell or transfer data to third-parties for the purposes he did. In doing so, Kogan and his company violated Facebook's Platform Policies.

On December 11, 2015, *The Guardian* published an article reporting that Kogan and his company, GSR, may have passed information the app had obtained from Facebook users to SCL Elections Ltd. (SCL)/Cambridge Analytica. Facebook immediately banned Kogan's app from our platform and investigated what happened and what further action Facebook should take to enforce our Platform Policies. Facebook considered the matter closed after obtaining written certifications and confirmations from Kogan, GSR, Cambridge Analytica, and SCL declaring that all such data they had obtained was accounted for and destroyed. We did not have any reason to affirmatively question the veracity of any of these certifications until March 2018, when we learned from media reporting that questions had been raised concerning the accuracy of the certifications. Facebook immediately banned Cambridge Analytica and SCL from purchasing advertisements on our services as well as removed the personal accounts of some of their officers. Moreover, while Facebook's policies in place at the time allowed us to audit apps to

ensure that they were safe and did not violate its terms, we had already terminated Kogan's app's access to Facebook. Accordingly, there were no ongoing concerns about the level of data that app could access or might access in the future. With the benefit of hindsight, we wish we had notified people whose information may have been impacted. Facebook has since notified all people potentially impacted with a detailed notice at the top of their News Feed.

416. How do you take responsibility for the result of the national election of 2016 after all your users' info on Facebook had been used to manipulate the election?

a. How will you prevent the same thing from happening again?

b. Please explain why you and other exec's of Facebook had had the liberty to delete (or unsend) your own messages and yet you hadn't allowed any other people on Facebook to do the same? What other liberties do you or other execs have in terms of privacy and security while all the other people don't or didn't (considering you'll fix those unfair issues)?

c. Please tell us what you are going to do specifically to gain back our trust because right now many people don't trust you or your company. Thank you.

We want our platform to be a place where people can have authentic conversations about elections and other political topics. We believe this kind of engagement promotes democracy, but we know that there are actors working to interfere with those conversations and undermine our elections. We are already taking steps to proactively prevent election interference and we are strengthening these protections going forward.

Engagement with campaigns: We want all candidates, groups, and voters to use our platform to engage in elections. We want it to be easy for people to find, follow, and contact their elected representatives—and those running to represent them. That's why, for candidates across the political spectrum, Facebook offers the same levels of support in key moments to help campaigns understand how best to use the platform. Both the Obama and Romney campaigns had access to the same tools, and no campaign received any special treatment from Facebook. Likewise, we offered identical support to both the Trump and Clinton campaigns, and had teams assigned to both. Everyone had access to the same tools, which are the same tools that every campaign is offered, and is consistent with support provided to commercial clients in the normal course of business. Facebook representatives advise political advertisers on Facebook, as they would with other, non-political managed accounts. We have a compliance team that trains our sales representatives to comply with all federal election law requirements in this area.

While no one from Facebook was assigned full-time to the Trump campaign, Facebook employees did interact with Cambridge Analytica employees. While our investigation is ongoing, our review indicates that Facebook employees did not identify any issues involving the improper use of Facebook data in the course of their interactions with Cambridge Analytica during the 2016 US Presidential campaign.

Election Integrity: In the run-up to the 2016 elections, we were focused on the kinds of cybersecurity attacks typically used by nation states, for example phishing and malware attacks. And we were too slow to spot information operations interference. Since then, we've made important changes to prevent bad actors from using misinformation to undermine the democratic process. This will never be a solved problem because we're up against determined, creative and well-funded adversaries. But we are making steady progress. Here is a list of the 10 most important changes we have made:

- **Ads transparency.** Advertising should be transparent: users should be able to see all the ads an advertiser is currently running on Facebook, Instagram and Messenger. And for ads with political content, we've created an archive that will hold ads with political content for seven years—including information about ad impressions and spend, as well as demographic data such as age, gender and location. People in Canada and Ireland have already been able to see all the ads that a Page is running on Facebook—and we've launched this globally.

- **Verification and labeling.** Every advertiser will now need to confirm their ID and location before being able to run any ads with political content in the US. All ads with political content will also clearly state who paid for them.

- **Updating targeting.** We want ads on Facebook to be safe and civil. We thoroughly review the targeting criteria advertisers can use to ensure they are consistent with our principles. As a result, we removed nearly one-third of the targeting segments used by the IRA. We continue to allow some criteria that people may find controversial. But we do see businesses marketing things like historical books, documentaries or television shows using them in legitimate ways.

- **Better technology.** Over the past year, we've gotten increasingly better at finding and disabling fake accounts. We now block millions of fake accounts each day as people try to create them—and before they've done any harm. This is thanks to improvements in machine learning and artificial intelligence, which can proactively identify suspicious behavior at a scale that was not possible before—without needing to look at the content itself.

- **Action to tackle fake news.** We are working hard to stop the spread of false news. We work with third-party fact-checking organizations to limit the spread of articles rated false. To reduce the spread of false news, we remove fake accounts and disrupt economic incentives for traffickers of misinformation. We also use various signals, including feedback from our community, to identify potential false news. In countries where we have partnerships with independent third-party fact-checkers, stories rated as false by those fact-checkers are shown lower in News Feed. If Pages or domains repeatedly create or share misinformation, we significantly reduce their distribution and remove their advertising rights. We also want to empower people to decide for themselves what to read, trust, and share. We promote news literacy and work to inform people with more context. For example, if third-party fact-checkers write articles about a news story, we show them immediately below the story in the Related Articles unit. We also notify people and Page Admins if they try to share a story, or have shared one in the past, that's

been determined to be false. In addition to our own efforts, we're learning from academics, scaling our partnerships with third-party fact-checkers and talking to other organizations about how we can work together.

A key focus is working to disrupt the economics of fake news. For example, preventing the creation of fake accounts that spread it, banning sites that engage in this behavior from using our ad products, and demoting articles found to be false by fact checkers in News Feed—causing it to lose 80% of its traffic. We now work with independent fact checkers in the US, France, Germany, Ireland, the Netherlands, Italy, Mexico, Colombia, India, Indonesia and the Philippines with plans to scale to more countries in the coming months.

- **Significant investments in security.** We're doubling the number of people working on safety and security from 10,000 last year to over 20,000 this year. We expect these investments to impact our profitability. But the safety of people using Facebook needs to come before profit.

- **Industry collaboration.** Recently, we joined 34 global tech and security companies in signing a TechAccord pact to help improve security for everyone.

- **Information sharing and reporting channels.** In the 2017 German elections, we worked closely with the authorities there, including the Federal Office for Information Security (BSI). This gave them a dedicated reporting channel for security issues related to the federal elections.

- **Tracking 40+ elections.** In recent months, we've started to deploy new tools and teams to proactively identify threats in the run-up to specific elections. We first tested this effort during the Alabama Senate election, and plan to continue these efforts for elections around the globe, including the US midterms. Last year we used public service announcements to help inform people about fake news in 21 separate countries, including in advance of French, Kenyan and German elections.

- **Action against the Russia-based IRA.** In April, we removed 70 Facebook and 65 Instagram accounts—as well as 138 Facebook Pages—controlled by the IRA primarily targeted either at people living in Russia or Russian-speakers around the world including from neighboring countries like Azerbaijan, Uzbekistan and Ukraine. The IRA has repeatedly used complex networks of inauthentic accounts to deceive and manipulate people in the US, Europe and Russia—and we don't want them on Facebook anywhere in the world.

417. How do I unsubscribe from Facebook? Bernie

We believe that it's important to communicate with people about the information that we collect and how people can control it. As explained in our Data Policy, we collect three basic categories of data about people:

(1) data about things people do and share (and who they connect with) on our services;

(2) data about the devices people use to access our services; and

(3) data we receive from partners, including the websites and apps that use our business tools.

We collect information about the people, Pages, accounts, hashtags, and groups users are connected to and how they interact with them across our Products, such as people a user communicates with the most or groups users are part of. We also collect contact information if they choose to upload, sync, or import it from a device (such as an address book or call log or SMS log history), which we use for things like helping them and others find people they may know.

The data we use to show ads to people depends on the data we have received from people. For people who are new to Facebook, we may have minimal data that we can use. For people who have used our services for longer, we likely have more data, but the amount of data will depend on the nature of that use and how they have used our controls. Any person can see each of the specific interests we maintain about them for advertising by visiting Ads Preferences, which lets people see what interests we use to choose ads for them—and to edit or delete these interests. We also provide more detailed information about how we use data to decide what ads to show to people in our "About Facebook Ads" page, at https://www.facebook.com/ads/about. And, we do not sell people's information to anyone, and we never will.

All users must expressly consent to Facebook's Terms and Data Policy when registering for Facebook. The Data Policy explains the kinds of information we collect, how we use this information, how we share this information, and how users can manage and delete information.

Facebook does not create profiles for people without a Facebook account, but we do receive some information from devices and browsers that may be used by non-users. For example:

- When people visit apps or websites that feature our technologies—like the Facebook Like or Comment button—our servers automatically log (i) standard browser or app records of the fact that a particular device or user visited the website or app (this connection to Facebook's servers occurs automatically when a person visits a website or app that contains our technologies, such as a Like button, and is an inherent function of Internet design); and (ii) any additional information the publisher of the app or website chooses to share with Facebook about the person's activities on that site (such as the fact that a purchase was made on the site). This is a standard feature of the Internet, and most websites and apps share this same information with multiple different third-parties whenever people visit their website or app. When the person visiting a website featuring Facebook's tools is not a registered Facebook user, Facebook does not have information identifying that individual, and it does not create profiles for this individual.

- We also may receive information about the device of a non-registered user if that user visits a part of Facebook that does not require people to log in—such as a public Facebook Page. The information we log when people visit our websites or apps is the

same as described above and is the same information that any provider of an online service would receive.

- In addition, Facebook may receive some basic information about devices where Facebook apps are installed, including before people using those devices have registered for Facebook (such as when a user downloads a Facebook app, but has not yet created an account, or if the app is preloaded on a given device). This device data includes things like device model, operating system, IP address, app version and device identifiers. We use this information to provide the right version of the app, help people who want to create accounts (for example, optimizing the registration flow for the specific device), retrieving bug fixes and measuring and improving app performance. We do not use this information to build profiles about non-registered users.

418. Before you had children yourself, did you care about how your greed would affect our children?

As discussed with your staff, this question is not germane to the hearing.

419. The Facebook application is presumably going to evolve, so what have you taken away from this episode with respect to being a socially responsible innovator?

We believe everyone deserves good privacy controls. A user owns the information they share on Facebook. This means they decide what they share and who they share it with on Facebook, and they can change their mind. We require websites and apps who use our tools to tell users they're collecting and sharing their information with us, and to get users' permission to do so.

Everyone has the right to expect strong protections for their information. We also need to do our part to help keep our community safe, in a way that's consistent with people's privacy expectations. We've recently announced several steps to give people more control over their privacy, including a new Privacy Shortcuts tool that we're rolling out now to give people information about how to control their information, including choosing who can see what they post and adding protections like two-factor authentication to their account. People can learn more about how to protect their privacy in our updated Data Policy and in our Privacy Basics feature (https://www.facebook.com/about/basics).

We are in the process of investigating every app that had access to a large amount of information before we changed our Platform in 2014. The investigation process is in full swing. We have large teams of internal and external experts working hard to investigate these apps as quickly as possible. As of early June 2018, thousands of apps have been investigated and around 200 apps have been suspended—pending a thorough investigation into whether they did in fact misuse any data. Where we find evidence that these or other apps did misuse data, we will ban them and let people know.

Facebook is generally not opposed to regulation but wants to ensure it is the right regulation. The issues facing the industry are complex, multi-faceted, and affect an important part of peoples' lives. As such, Facebook is absolutely committed to working with regulators,

like Congress, to craft the right regulations. Facebook would be happy to review any proposed legislation and provide comments.

420. I want to know if I was one who had her data stolen. If so I want reparation.

Facebook's policies regarding third-party usage of its platform technologies have prohibited—and continue to prohibit—third-party app developers from selling or licensing user data accessed from Facebook and from sharing any user data accessed from Facebook with any ad network, data broker or other advertising or monetization-related service. We take action on potential violations of our Platform Policies based on proactive review, external reports, and other signals. Kogan was not permitted to sell or transfer data to third-parties for the purposes he did. In doing so, Kogan and his company violated Facebook's Platform Policies.

On December 11, 2015, *The Guardian* published an article reporting that Kogan and his company, GSR, may have passed information the app had obtained from Facebook users to SCL Elections Ltd. (SCL)/Cambridge Analytica. Facebook immediately banned Kogan's app from our platform and investigated what happened and what further action Facebook should take to enforce our Platform Policies. Facebook considered the matter closed after obtaining written certifications and confirmations from Kogan, GSR, Cambridge Analytica, and SCL declaring that all such data they had obtained was accounted for and destroyed. We did not have any reason to affirmatively question the veracity of any of these certifications until March 2018, when we learned from media reporting that questions had been raised concerning the accuracy of the certifications. Facebook immediately banned Cambridge Analytica and SCL from purchasing advertisements on our services as well as removed the personal accounts of some of their officers. Moreover, while Facebook's policies in place at the time allowed us to audit apps to ensure that they were safe and did not violate its terms, we had already terminated Kogan's app's access to Facebook. Accordingly, there were no ongoing concerns about the level of data that app could access or might access in the future. With the benefit of hindsight, we wish we had notified people whose information may have been impacted. Facebook has since notified all people potentially impacted with a detailed notice at the top of their News Feed.

421. Sean Parker, Facebook's founding president, said last November that it is designed to be addictive, that it is intentionally "exploiting a vulnerability in human psychology". If Facebook is addictive by design, does that mean using it can be potentially self-destructive, like using any addictive product? Who should pay the costs of managing and treating addictions intentionally created by Facebook?

Facebook employs social psychologists, social scientists, and sociologists, and collaborates with top scholars to better understand well-being. Facebook has also pledged $1 million towards research to better understand the relationship between media technologies, youth development and well-being. Facebook is teaming up with experts in the field to look at the impact of mobile technology and social media on kids and teens, as well as how to better support them as they transition through different stages of life. Facebook is committed to bringing people together and supporting well-being through meaningful interactions on Facebook.

422. What has Facebook done to identify and assist users that exhibit compulsive or addictive behavior on your site?

Facebook employs social psychologists, social scientists, and sociologists, and collaborates with top scholars to better understand well-being. Facebook has also pledged $1 million towards research to better understand the relationship between media technologies, youth development and well-being. Facebook is teaming up with experts in the field to look at the impact of mobile technology and social media on kids and teens, as well as how to better support them as they transition through different stages of life. Facebook is committed to bringing people together and supporting well-being through meaningful interactions on Facebook.

423. How much are you going to pay everyone who had their data stolen? Sorry will just not cut it.

Facebook's policies regarding third-party usage of its platform technologies have prohibited—and continue to prohibit—third-party app developers from selling or licensing user data accessed from Facebook and from sharing any user data accessed from Facebook with any ad network, data broker or other advertising or monetization-related service. We take action on potential violations of our Platform Policies based on proactive review, external reports, and other signals. Kogan was not permitted to sell or transfer data to third-parties for the purposes he did. In doing so, Kogan and his company violated Facebook's Platform Policies.

On December 11, 2015, *The Guardian* published an article reporting that Kogan and his company, GSR, may have passed information the app had obtained from Facebook users to SCL Elections Ltd. (SCL)/Cambridge Analytica. Facebook immediately banned Kogan's app from our platform and investigated what happened and what further action Facebook should take to enforce our Platform Policies. Facebook considered the matter closed after obtaining written certifications and confirmations from Kogan, GSR, Cambridge Analytica, and SCL declaring that all such data they had obtained was accounted for and destroyed. We did not have any reason to affirmatively question the veracity of any of these certifications until March 2018, when we learned from media reporting that questions had been raised concerning the accuracy of the certifications. Facebook immediately banned Cambridge Analytica and SCL from purchasing advertisements on our services as well as removed the personal accounts of some of their officers. Moreover, while Facebook's policies in place at the time allowed us to audit apps to ensure that they were safe and did not violate its terms, we had already terminated Kogan's app's access to Facebook. Accordingly, there were no ongoing concerns about the level of data that app could access or might access in the future. With the benefit of hindsight, we wish we had notified people whose information may have been impacted. Facebook has since notified all people potentially impacted with a detailed notice at the top of their News Feed.

424. How will Facebook address the "affiliates" problem? (See Bloomberg Businessweek, April 2, 2018. p56

As discussed with your staff, this question is not germane to the hearing.

425. A fundamental bias on your part appears to be that users bear some responsibility for their own protection from bad actors. Yet it seems clear that a sizable percentage of your user population lacks the cognitive abilities, skills and training necessary for successful self-protection online. How do you propose that these users should proceed?

We believe that it's important to communicate with people about the information that we collect and how people can control it. As explained in our Data Policy, we collect three basic categories of data about people:

(1) data about things people do and share (and who they connect with) on our services;

(2) data about the devices people use to access our services; and

(3) data we receive from partners, including the websites and apps that use our business tools.

We collect information about the people, Pages, accounts, hashtags, and groups users are connected to and how they interact with them across our Products, such as people a user communicates with the most or groups users are part of. We also collect contact information if they choose to upload, sync, or import it from a device (such as an address book or call log or SMS log history), which we use for things like helping them and others find people they may know.

The data we use to show ads to people depends on the data we have received from people. For people who are new to Facebook, we may have minimal data that we can use. For people who have used our services for longer, we likely have more data, but the amount of data will depend on the nature of that use and how they have used our controls. Any person can see each of the specific interests we maintain about them for advertising by visiting Ads Preferences, which lets people see what interests we use to choose ads for them—and to edit or delete these interests. We also provide more detailed information about how we use data to decide what ads to show to people in our "About Facebook Ads" page, at https://www.facebook.com/ads/about. And, we do not sell people's information to anyone, and we never will.

All users must expressly consent to Facebook's Terms and Data Policy when registering for Facebook. The Data Policy explains the kinds of information we collect, how we use this information, how we share this information, and how users can manage and delete information.

Facebook does not create profiles for people without a Facebook account, but we do receive some information from devices and browsers that may be used by non-users. For example:

- When people visit apps or websites that feature our technologies—like the Facebook Like or Comment button—our servers automatically log (i) standard browser or app records of the fact that a particular device or user visited the website or app (this connection to Facebook's servers occurs automatically when a person visits a website or app that contains our technologies, such as a Like button, and is an inherent function of Internet design); and (ii) any additional information the publisher of the app or website chooses to share with Facebook about the person's activities on that site (such as the fact that a purchase was made on the site). This is a standard feature of the Internet, and most websites and apps share this same information with multiple different third-parties whenever people visit their website or app. When the person visiting a website featuring

Facebook's tools is not a registered Facebook user, Facebook does not have information identifying that individual, and it does not create profiles for this individual.

- We also may receive information about the device of a non-registered user if that user visits a part of Facebook that does not require people to log in—such as a public Facebook Page. The information we log when people visit our websites or apps is the same as described above and is the same information that any provider of an online service would receive.

- In addition, Facebook may receive some basic information about devices where Facebook apps are installed, including before people using those devices have registered for Facebook (such as when a user downloads a Facebook app, but has not yet created an account, or if the app is preloaded on a given device). This device data includes things like device model, operating system, IP address, app version and device identifiers. We use this information to provide the right version of the app, help people who want to create accounts (for example, optimizing the registration flow for the specific device), retrieving bug fixes and measuring and improving app performance. We do not use this information to build profiles about non-registered users.

426. Social responsibility to our children—increasing signs of mental distress from SM?

Protecting people's data is one of our most important responsibilities, and we are committed to continuing our work to improve how we protect people's information and to working with regulators to draft appropriate regulations. Our mission is to give people the power to build community and bring the world closer together. As the internet becomes more important in people's lives, the real question is about the right set of regulations that should apply to all internet services, regardless of size. Across the board, we have a responsibility to not just build tools, but to make sure that they're used in ways that are positive for our users. Facebook is generally not opposed to regulation but wants to ensure it is the right regulation. The issues facing the industry are complex, multi-faceted, and affect an important part of peoples' lives. As such, Facebook is absolutely committed to working with regulators, like Congress, to craft the right regulations.

We are already regulated in many ways—for example, under the Federal Trade Commission Act—and we are subject to ongoing oversight by the FTC under the terms of a 2011 consent order. We furnished extensive information to the FTC regarding the ability for users to port their Facebook data (including friends data that had been shared with them) with apps on Facebook's platform, as part of the FTC's investigation culminating in the July 27, 2012 Consent Order. The Consent Order memorializes the agreement between Facebook and the FTC and did not require Facebook to turn off or change the ability for people to port friends data that had been shared with them on Facebook to apps they used. Facebook voluntarily changed this feature of Platform in 2014, however. Facebook has not violated the Federal Trade Commission Act. Facebook is not in a position to determine whether third-party app developers violated the Act and leaves that determination to the FTC, although we can confirm that misrepresenting the terms of an app to users is a violation of Facebook's developer policies.

Facebook has inherent incentives to protect its customers' privacy and address breaches and vulnerabilities. Indeed, the recent discovery of misconduct by an app developer on the Facebook platform clearly hurt Facebook and made it harder for us to achieve our social mission. As such, Facebook is committed to protecting our platform from bad actors, ensuring we are able to continue our mission of giving people a voice and bringing them closer together. It will take some time to work through all the changes we need to make across the company, but Facebook is committed to getting this right.

427. How do you confirm who is paying you for information?

Facebook's policies regarding third-party usage of its platform technologies have prohibited—and continue to prohibit—third-party app developers from selling or licensing user data obtained from Facebook and from sharing any user data obtained from Facebook with any ad network, data broker or other advertising or monetization-related service.

We use a variety of tools to enforce Facebook policies against violating parties, including developers. We review tens of thousands of apps per year and regularly disapprove noncompliant apps as part of our proactive review process. We also use tools like cease and desist letters, account suspensions, letter agreements, and civil litigation. For example, since 2006, Facebook has sent over 1,150 cease-and-desist letters to over 1,600 targets. In 2017, we took action against about 370,000 apps, ranging from imposing certain restrictions to removal of the app from the platform. Moreover, we have required parties who have procured our data without authorization to delete that data. We have invested significant resources in these efforts.

Recently, we announced a number of additional steps we're taking to address concerns raised by Kogan's app.

- **Review our platform.** We will investigate all apps that had access to large amounts of data before the platform changes we announced in 2014, and we will audit any app where we identify suspicious activity. If we identify misuses of data, we'll take immediate action, including banning the app from our platform and pursuing legal action if appropriate.

- **Tell people about data misuse.** We will tell people about apps that have misused their data. This includes building a way for people to know if their data might have been accessed via the app. Moving forward, if we remove an app, we will tell people.

- **Turn off access for unused apps.** If someone has not used an app within the last three months, we will turn off the app's access to their data.

- **Restrict Facebook Login data.** We are changing Login, so that the only data that an app can request without app review will include name, profile photo, and email address. Requesting any other data will require approval from Facebook. We will also no longer allow apps to ask for access to information like religious or political views, relationship status and details, custom friends lists, education and work history, fitness activity, book reading and music listening activity, news reading, video watch activity, and games activity. We will encourage people to manage the apps they use. We already show people

what apps their accounts are connected to and allow them to control what data they've permitted those apps to use. But we're making it easier for people to see what apps they use and the information they have shared with those apps.

- **Reward people who find vulnerabilities.** We launched the Data Abuse Bounty program so that people can report to us any misuses of data by app developers.

- **Update our policies.** We have updated our terms and Data Policy to explain how we use data and how data is shared with app developers.

428. What steps are you taking to verify what clients tell you?

Facebook's policies regarding third-party usage of its platform technologies have prohibited—and continue to prohibit—third-party app developers from selling or licensing user data obtained from Facebook and from sharing any user data obtained from Facebook with any ad network, data broker or other advertising or monetization-related service.

We use a variety of tools to enforce Facebook policies against violating parties, including developers. We review tens of thousands of apps per year and regularly disapprove noncompliant apps as part of our proactive review process. We also use tools like cease and desist letters, account suspensions, letter agreements, and civil litigation. For example, since 2006, Facebook has sent over 1,150 cease-and-desist letters to over 1,600 targets. In 2017, we took action against about 370,000 apps, ranging from imposing certain restrictions to removal of the app from the platform. Moreover, we have required parties who have procured our data without authorization to delete that data. We have invested significant resources in these efforts.

Recently, we announced a number of additional steps we're taking to address concerns raised by Kogan's app.

- **Review our platform.** We will investigate all apps that had access to large amounts of data before the platform changes we announced in 2014, and we will audit any app where we identify suspicious activity. If we identify misuses of data, we'll take immediate action, including banning the app from our platform and pursuing legal action if appropriate.

- **Tell people about data misuse.** We will tell people about apps that have misused their data. This includes building a way for people to know if their data might have been accessed via the app. Moving forward, if we remove an app, we will tell people.

- **Turn off access for unused apps.** If someone has not used an app within the last three months, we will turn off the app's access to their data.

- **Restrict Facebook Login data.** We are changing Login, so that the only data that an app can request without app review will include name, profile photo, and email address. Requesting any other data will require approval from Facebook. We will also no longer allow apps to ask for access to information like religious or political views, relationship status and details, custom friends lists, education and work history, fitness activity, book

reading and music listening activity, news reading, video watch activity, and games activity. We will encourage people to manage the apps they use. We already show people what apps their accounts are connected to and allow them to control what data they've permitted those apps to use. But we're making it easier for people to see what apps they use and the information they have shared with those apps.

- **Reward people who find vulnerabilities.** We launched the Data Abuse Bounty program so that people can report to us any misuses of data by app developers.

- **Update our policies.** We have updated our terms and Data Policy to explain how we use data and how data is shared with app developers.

429. Why was it OK when President Obama's team downloaded user earlier. No problem until it is public.

We want our platform to be a place where people can have authentic conversations about elections and other political topics. We believe this kind of engagement promotes democracy, but we know that there are actors working to interfere with those conversations and undermine our elections. We are already taking steps to proactively prevent election interference and we are strengthening these protections going forward.

Engagement with campaigns: We want all candidates, groups, and voters to use our platform to engage in elections. We want it to be easy for people to find, follow, and contact their elected representatives—and those running to represent them. That's why, for candidates across the political spectrum, Facebook offers the same levels of support in key moments to help campaigns understand how best to use the platform. Both the Obama and Romney campaigns had access to the same tools, and no campaign received any special treatment from Facebook. Likewise, we offered identical support to both the Trump and Clinton campaigns, and had teams assigned to both. Everyone had access to the same tools, which are the same tools that every campaign is offered, and is consistent with support provided to commercial clients in the normal course of business. Facebook representatives advise political advertisers on Facebook, as they would with other, non-political managed accounts. We have a compliance team that trains our sales representatives to comply with all federal election law requirements in this area.

While no one from Facebook was assigned full-time to the Trump campaign, Facebook employees did interact with Cambridge Analytica employees. While our investigation is ongoing, our review indicates that Facebook employees did not identify any issues involving the improper use of Facebook data in the course of their interactions with Cambridge Analytica during the 2016 US Presidential campaign.

Election Integrity: In the run-up to the 2016 elections, we were focused on the kinds of cybersecurity attacks typically used by nation states, for example phishing and malware attacks. And we were too slow to spot information operations interference. Since then, we've made important changes to prevent bad actors from using misinformation to undermine the democratic process. This will never be a solved problem because we're up against determined, creative and well-funded adversaries. But we are making steady progress. Here is a list of the 10 most important changes we have made:

- **Ads transparency.** Advertising should be transparent: users should be able to see all the ads an advertiser is currently running on Facebook, Instagram and Messenger. And for ads with political content, we've created an archive that will hold ads with political content for seven years—including information about ad impressions and spend, as well as demographic data such as age, gender and location. People in Canada and Ireland have already been able to see all the ads that a Page is running on Facebook—and we've launched this globally.

- **Verification and labeling.** Every advertiser will now need to confirm their ID and location before being able to run any ads with political content in the US. All ads with political content will also clearly state who paid for them.

- **Updating targeting.** We want ads on Facebook to be safe and civil. We thoroughly review the targeting criteria advertisers can use to ensure they are consistent with our principles. As a result, we removed nearly one-third of the targeting segments used by the IRA. We continue to allow some criteria that people may find controversial. But we do see businesses marketing things like historical books, documentaries or television shows using them in legitimate ways.

- **Better technology.** Over the past year, we've gotten increasingly better at finding and disabling fake accounts. We now block millions of fake accounts each day as people try to create them—and before they've done any harm. This is thanks to improvements in machine learning and artificial intelligence, which can proactively identify suspicious behavior at a scale that was not possible before—without needing to look at the content itself.

- **Action to tackle fake news.** We are working hard to stop the spread of false news. We work with third-party fact-checking organizations to limit the spread of articles rated false. To reduce the spread of false news, we remove fake accounts and disrupt economic incentives for traffickers of misinformation. We also use various signals, including feedback from our community, to identify potential false news. In countries where we have partnerships with independent third-party fact-checkers, stories rated as false by those fact-checkers are shown lower in News Feed. If Pages or domains repeatedly create or share misinformation, we significantly reduce their distribution and remove their advertising rights. We also want to empower people to decide for themselves what to read, trust, and share. We promote news literacy and work to inform people with more context. For example, if third-party fact-checkers write articles about a news story, we show them immediately below the story in the Related Articles unit. We also notify people and Page Admins if they try to share a story, or have shared one in the past, that's been determined to be false. In addition to our own efforts, we're learning from academics, scaling our partnerships with third-party fact-checkers and talking to other organizations about how we can work together.

  A key focus is working to disrupt the economics of fake news. For example, preventing the creation of fake accounts that spread it, banning sites that engage in this behavior from using our ad products, and demoting articles found to be false by fact checkers in

News Feed—causing it to lose 80% of its traffic. We now work with independent fact checkers in the US, France, Germany, Ireland, the Netherlands, Italy, Mexico, Colombia, India, Indonesia and the Philippines with plans to scale to more countries in the coming months.

- **Significant investments in security.** We're doubling the number of people working on safety and security from 10,000 last year to over 20,000 this year. We expect these investments to impact our profitability. But the safety of people using Facebook needs to come before profit.

- **Industry collaboration.** Recently, we joined 34 global tech and security companies in signing a TechAccord pact to help improve security for everyone.

- **Information sharing and reporting channels.** In the 2017 German elections, we worked closely with the authorities there, including the Federal Office for Information Security (BSI). This gave them a dedicated reporting channel for security issues related to the federal elections.

- **Tracking 40+ elections.** In recent months, we've started to deploy new tools and teams to proactively identify threats in the run-up to specific elections. We first tested this effort during the Alabama Senate election, and plan to continue these efforts for elections around the globe, including the US midterms. Last year we used public service announcements to help inform people about fake news in 21 separate countries, including in advance of French, Kenyan and German elections.

- **Action against the Russia-based IRA.** In April, we removed 70 Facebook and 65 Instagram accounts—as well as 138 Facebook Pages—controlled by the IRA primarily targeted either at people living in Russia or Russian-speakers around the world including from neighboring countries like Azerbaijan, Uzbekistan and Ukraine. The IRA has repeatedly used complex networks of inauthentic accounts to deceive and manipulate people in the US, Europe and Russia—and we don't want them on Facebook anywhere in the world.

430. When will he be stepping down?

We recognize that we have made mistakes, and we are committed to learning from this experience to secure our platform further and make our community safer for everyone going forward. As our CEO Mark Zuckerberg has said, when you are building something unprecedented like Facebook, there are going to be mistakes. What people should hold us accountable for is learning from the mistakes and continually doing better—and, at the end of the day, making sure that we're building things that people like and that make their lives better.

Particularly in the past few months, we've realized that we need to take a broader view of our responsibility to our community. Part of that effort is continuing our ongoing efforts to identify ways that we can improve our privacy practices. We've heard loud and clear that privacy settings and other important tools are too hard to find and that we must do more to keep people informed. So, we're taking additional steps to put people more in control of their privacy. For

instance, we redesigned our entire settings menu on mobile devices from top to bottom to make things easier to find. We also created a new Privacy Shortcuts in a menu where users can control their data in just a few taps, with clearer explanations of how our controls work. The experience is now clearer, more visual, and easy-to-find. Furthermore, we also updated our terms of service that include our commitments to everyone using Facebook. We explain the services we offer in language that's easier to read. We've also updated our Data Policy to better spell out what data we collect and how we use it in Facebook, Instagram, Messenger, and other products.

431. Will we continue believing that one man can fix this? A convenient narrative that allows us to duck

As discussed with your staff, this question is not germane to the hearing.

432. Mr. Zuckerberg, what bad thing will really happen because of this data breach?

Facebook's policies regarding third-party usage of its platform technologies have prohibited—and continue to prohibit—third-party app developers from selling or licensing user data accessed from Facebook and from sharing any user data accessed from Facebook with any ad network, data broker or other advertising or monetization-related service. We take action on potential violations of our Platform Policies based on proactive review, external reports, and other signals. Kogan was not permitted to sell or transfer data to third-parties for the purposes he did. In doing so, Kogan and his company violated Facebook's Platform Policies.

On December 11, 2015, *The Guardian* published an article reporting that Kogan and his company, GSR, may have passed information the app had obtained from Facebook users to SCL Elections Ltd. (SCL)/Cambridge Analytica. Facebook immediately banned Kogan's app from our platform and investigated what happened and what further action Facebook should take to enforce our Platform Policies. Facebook considered the matter closed after obtaining written certifications and confirmations from Kogan, GSR, Cambridge Analytica, and SCL declaring that all such data they had obtained was accounted for and destroyed. We did not have any reason to affirmatively question the veracity of any of these certifications until March 2018, when we learned from media reporting that questions had been raised concerning the accuracy of the certifications. Facebook immediately banned Cambridge Analytica and SCL from purchasing advertisements on our services as well as removed the personal accounts of some of their officers. Moreover, while Facebook's policies in place at the time allowed us to audit apps to ensure that they were safe and did not violate its terms, we had already terminated Kogan's app's access to Facebook. Accordingly, there were no ongoing concerns about the level of data that app could access or might access in the future. With the benefit of hindsight, we wish we had notified people whose information may have been impacted. Facebook has since notified all people potentially impacted with a detailed notice at the top of their News Feed.

433. Good luck. He will make the senate/congress look buffoonish. He has already done in Menlo Park

As discussed with your staff, this question is not germane to the hearing.

434. Mr. Zuckerberg, what protections do use for your personal information? Should your user expect less?

We believe everyone deserves good privacy controls. A user owns the information they share on Facebook. This means they decide what they share and who they share it with on Facebook, and they can change their mind. We require websites and apps who use our tools to tell users they're collecting and sharing their information with us, and to get users' permission to do so.

Everyone has the right to expect strong protections for their information. We also need to do our part to help keep our community safe, in a way that's consistent with people's privacy expectations. We've recently announced several steps to give people more control over their privacy, including a new Privacy Shortcuts tool that we're rolling out now to give people information about how to control their information, including choosing who can see what they post and adding protections like two-factor authentication to their account. People can learn more about how to protect their privacy in our updated Data Policy and in our Privacy Basics feature (https://www.facebook.com/about/basics).

We are in the process of investigating every app that had access to a large amount of information before we changed our Platform in 2014. The investigation process is in full swing. We have large teams of internal and external experts working hard to investigate these apps as quickly as possible. As of early June 2018, thousands of apps have been investigated and around 200 apps have been suspended—pending a thorough investigation into whether they did in fact misuse any data. Where we find evidence that these or other apps did misuse data, we will ban them and let people know.

Facebook is generally not opposed to regulation but wants to ensure it is the right regulation. The issues facing the industry are complex, multi-faceted, and affect an important part of peoples' lives. As such, Facebook is absolutely committed to working with regulators, like Congress, to craft the right regulations. Facebook would be happy to review any proposed legislation and provide comments.

435. After tragic consequences from bullying on FB emerged, how is it possible that FB failed to look for other forms of manipulation based on feeding human prejudices?

Freedom of expression is one of our core values, and we believe that adding voices to the conversation creates a richer and more vibrant community. We want people to feel confident that our community welcomes all viewpoints and we are committed to designing our products to give all people a voice and foster the free flow of ideas and culture. We recognize how important it is for Facebook to be a place where people feel empowered to communicate, and we take our role in keeping abuse off our service seriously. Our mission entails embracing diverse views. We err on the side of allowing content, even when some find it objectionable, unless removing that content prevents a specific harm.

However, we are, first and foremost, a technology company. Facebook does not create or edit the content that our users post on our platform. While we seek to be a platform for a broad range of ideas, we do moderate content in good faith according to published community standards in order to keep users on the platform safe, reduce objectionable content and to make sure users participate on the platform responsibly.

436. Do you understand how offensive Facebook's actions have been to users?

Facebook's policies regarding third-party usage of its platform technologies have prohibited—and continue to prohibit—third-party app developers from selling or licensing user data accessed from Facebook and from sharing any user data accessed from Facebook with any ad network, data broker or other advertising or monetization-related service. We take action on potential violations of our Platform Policies based on proactive review, external reports, and other signals. Kogan was not permitted to sell or transfer data to third-parties for the purposes he did. In doing so, Kogan and his company violated Facebook's Platform Policies.

On December 11, 2015, *The Guardian* published an article reporting that Kogan and his company, GSR, may have passed information the app had obtained from Facebook users to SCL Elections Ltd. (SCL)/Cambridge Analytica. Facebook immediately banned Kogan's app from our platform and investigated what happened and what further action Facebook should take to enforce our Platform Policies. Facebook considered the matter closed after obtaining written certifications and confirmations from Kogan, GSR, Cambridge Analytica, and SCL declaring that all such data they had obtained was accounted for and destroyed. We did not have any reason to affirmatively question the veracity of any of these certifications until March 2018, when we learned from media reporting that questions had been raised concerning the accuracy of the certifications. Facebook immediately banned Cambridge Analytica and SCL from purchasing advertisements on our services as well as removed the personal accounts of some of their officers. Moreover, while Facebook's policies in place at the time allowed us to audit apps to ensure that they were safe and did not violate its terms, we had already terminated Kogan's app's access to Facebook. Accordingly, there were no ongoing concerns about the level of data that app could access or might access in the future. With the benefit of hindsight, we wish we had notified people whose information may have been impacted. Facebook has since notified all people potentially impacted with a detailed notice at the top of their News Feed.

437. Give him an example if you can, of how a family could be affected by the way he operates without it.

As discussed with your staff, this question is not germane to the hearing.

438. Why is it not morally and ethically repugnant to you to sell the personal data of your customer?

We believe that it's important to communicate with people about the information that we collect and how people can control it. As explained in our Data Policy, we collect three basic categories of data about people:

(1) data about things people do and share (and who they connect with) on our services;

(2) data about the devices people use to access our services; and

(3) data we receive from partners, including the websites and apps that use our business tools.

We collect information about the people, Pages, accounts, hashtags, and groups users are connected to and how they interact with them across our Products, such as people a user communicates with the most or groups users are part of. We also collect contact information if they choose to upload, sync, or import it from a device (such as an address book or call log or SMS log history), which we use for things like helping them and others find people they may know.

The data we use to show ads to people depends on the data we have received from people. For people who are new to Facebook, we may have minimal data that we can use. For people who have used our services for longer, we likely have more data, but the amount of data will depend on the nature of that use and how they have used our controls. Any person can see each of the specific interests we maintain about them for advertising by visiting Ads Preferences, which lets people see what interests we use to choose ads for them—and to edit or delete these interests. We also provide more detailed information about how we use data to decide what ads to show to people in our "About Facebook Ads" page, at https://www.facebook.com/ads/about. And, we do not sell people's information to anyone, and we never will.

All users must expressly consent to Facebook's Terms and Data Policy when registering for Facebook. The Data Policy explains the kinds of information we collect, how we use this information, how we share this information, and how users can manage and delete information.

Facebook does not create profiles for people without a Facebook account, but we do receive some information from devices and browsers that may be used by non-users. For example:

- When people visit apps or websites that feature our technologies—like the Facebook Like or Comment button—our servers automatically log (i) standard browser or app records of the fact that a particular device or user visited the website or app (this connection to Facebook's servers occurs automatically when a person visits a website or app that contains our technologies, such as a Like button, and is an inherent function of Internet design); and (ii) any additional information the publisher of the app or website chooses to share with Facebook about the person's activities on that site (such as the fact that a purchase was made on the site). This is a standard feature of the Internet, and most websites and apps share this same information with multiple different third-parties whenever people visit their website or app. When the person visiting a website featuring Facebook's tools is not a registered Facebook user, Facebook does not have information identifying that individual, and it does not create profiles for this individual.

- We also may receive information about the device of a non-registered user if that user visits a part of Facebook that does not require people to log in—such as a public Facebook Page. The information we log when people visit our websites or apps is the same as described above and is the same information that any provider of an online service would receive.

- In addition, Facebook may receive some basic information about devices where Facebook apps are installed, including before people using those devices have registered for Facebook (such as when a user downloads a Facebook app, but has not yet created an

account, or if the app is preloaded on a given device). This device data includes things like device model, operating system, IP address, app version and device identifiers. We use this information to provide the right version of the app, help people who want to create accounts (for example, optimizing the registration flow for the specific device), retrieving bug fixes and measuring and improving app performance. We do not use this information to build profiles about non-registered users.

439. How can a user who is locked out of their email and change phone number close their account?

We believe that it's important to communicate with people about the information that we collect and how people can control it. As explained in our Data Policy, we collect three basic categories of data about people:

(1) data about things people do and share (and who they connect with) on our services;

(2) data about the devices people use to access our services; and

(3) data we receive from partners, including the websites and apps that use our business tools.

We collect information about the people, Pages, accounts, hashtags, and groups users are connected to and how they interact with them across our Products, such as people a user communicates with the most or groups users are part of. We also collect contact information if they choose to upload, sync, or import it from a device (such as an address book or call log or SMS log history), which we use for things like helping them and others find people they may know.

The data we use to show ads to people depends on the data we have received from people. For people who are new to Facebook, we may have minimal data that we can use. For people who have used our services for longer, we likely have more data, but the amount of data will depend on the nature of that use and how they have used our controls. Any person can see each of the specific interests we maintain about them for advertising by visiting Ads Preferences, which lets people see what interests we use to choose ads for them—and to edit or delete these interests. We also provide more detailed information about how we use data to decide what ads to show to people in our "About Facebook Ads" page, at https://www.facebook.com/ads/about. And, we do not sell people's information to anyone, and we never will.

All users must expressly consent to Facebook's Terms and Data Policy when registering for Facebook. The Data Policy explains the kinds of information we collect, how we use this information, how we share this information, and how users can manage and delete information.

Facebook does not create profiles for people without a Facebook account, but we do receive some information from devices and browsers that may be used by non-users. For example:

- When people visit apps or websites that feature our technologies—like the Facebook Like or Comment button—our servers automatically log (i) standard browser or app records of

the fact that a particular device or user visited the website or app (this connection to Facebook's servers occurs automatically when a person visits a website or app that contains our technologies, such as a Like button, and is an inherent function of Internet design); and (ii) any additional information the publisher of the app or website chooses to share with Facebook about the person's activities on that site (such as the fact that a purchase was made on the site). This is a standard feature of the Internet, and most websites and apps share this same information with multiple different third-parties whenever people visit their website or app. When the person visiting a website featuring Facebook's tools is not a registered Facebook user, Facebook does not have information identifying that individual, and it does not create profiles for this individual.

- We also may receive information about the device of a non-registered user if that user visits a part of Facebook that does not require people to log in—such as a public Facebook Page. The information we log when people visit our websites or apps is the same as described above and is the same information that any provider of an online service would receive.

- In addition, Facebook may receive some basic information about devices where Facebook apps are installed, including before people using those devices have registered for Facebook (such as when a user downloads a Facebook app, but has not yet created an account, or if the app is preloaded on a given device). This device data includes things like device model, operating system, IP address, app version and device identifiers. We use this information to provide the right version of the app, help people who want to create accounts (for example, optimizing the registration flow for the specific device), retrieving bug fixes and measuring and improving app performance. We do not use this information to build profiles about non-registered users.

440. Hi, Anna - Sylvia's daughter Diana here. I think the only thing I can think to ask is "Why?"

As discussed with your staff, this question is not germane to the hearing.

441. Can hacks be reduced if servers encoded time, location and IP addresses on each message?

For years, we had been aware of other types of activity that appeared to come from Russian sources—largely traditional security threats such as attacking people's accounts or using social media platforms to spread stolen information. What we saw early in the 2016 campaign cycle followed this pattern. Our security team that focuses on threat intelligence—which investigates advanced security threats as part of our overall information security organization—was, from the outset, alert to the possibility of Russian activity. In several instances before November 8, 2016, this team detected and mitigated threats from actors with ties to Russia and reported them to US law enforcement officials. This included activity from a cluster of accounts we had assessed to belong to a group (APT28) that the US government has publicly linked to Russian military intelligence services. This activity, which was aimed at employees of major US political parties, fell into the normal categories of offensive cyber activities we monitor for. We

warned the targets who were at highest risk, and were later in contact with law enforcement authorities about this activity.

Later in the summer we also started to see a new kind of behavior from APT28-related accounts—namely, the creation of fake personas that were then used to seed stolen information to journalists. These fake personas were organized under the banner of an organization that called itself DC Leaks. This activity violated our policies, and we removed the DC Leaks accounts.

Facebook learned from press accounts and statements by congressional leaders that Russian actors might have tried to interfere in the 2016 election by exploiting Facebook's ad tools. This is not something we had seen before, and so we started an investigation. We found that fake accounts associated with the IRA tried to influence the election.

This will never be a solved problem because we're up against determined, creative and well-funded adversaries. But we are making steady progress in preventing bad actors from using misinformation to undermine the democratic process, such as: increased ad transparency, advertiser verification and labeling, updating targeting criteria, better technological efforts to find and disable fake accounts, third-party fact checking to stop the spread of false news, doubling the number of people working on safety and security, greater industry collaboration, increased information sharing and reporting channels, proactive identification of election threats, and specific action against the Russia-based IRA.

We will continue to work with the government, and across the tech industry and civil society, to address this important national security matter so that we can do our part to prevent similar abuse from happening again.

442. Why is it so difficult for a user to cancel Facebook?

We believe that it's important to communicate with people about the information that we collect and how people can control it. As explained in our Data Policy, we collect three basic categories of data about people:

(1) data about things people do and share (and who they connect with) on our services;

(2) data about the devices people use to access our services; and

(3) data we receive from partners, including the websites and apps that use our business tools.

We collect information about the people, Pages, accounts, hashtags, and groups users are connected to and how they interact with them across our Products, such as people a user communicates with the most or groups users are part of. We also collect contact information if they choose to upload, sync, or import it from a device (such as an address book or call log or SMS log history), which we use for things like helping them and others find people they may know.

The data we use to show ads to people depends on the data we have received from people. For people who are new to Facebook, we may have minimal data that we can use. For people who have used our services for longer, we likely have more data, but the amount of data will depend on the nature of that use and how they have used our controls. Any person can see each of the specific interests we maintain about them for advertising by visiting Ads Preferences, which lets people see what interests we use to choose ads for them—and to edit or delete these interests. We also provide more detailed information about how we use data to decide what ads to show to people in our "About Facebook Ads" page, at https://www.facebook.com/ads/about. And, we do not sell people's information to anyone, and we never will.

All users must expressly consent to Facebook's Terms and Data Policy when registering for Facebook. The Data Policy explains the kinds of information we collect, how we use this information, how we share this information, and how users can manage and delete information.

Facebook does not create profiles for people without a Facebook account, but we do receive some information from devices and browsers that may be used by non-users. For example:

- When people visit apps or websites that feature our technologies—like the Facebook Like or Comment button—our servers automatically log (i) standard browser or app records of the fact that a particular device or user visited the website or app (this connection to Facebook's servers occurs automatically when a person visits a website or app that contains our technologies, such as a Like button, and is an inherent function of Internet design); and (ii) any additional information the publisher of the app or website chooses to share with Facebook about the person's activities on that site (such as the fact that a purchase was made on the site). This is a standard feature of the Internet, and most websites and apps share this same information with multiple different third-parties whenever people visit their website or app. When the person visiting a website featuring Facebook's tools is not a registered Facebook user, Facebook does not have information identifying that individual, and it does not create profiles for this individual.

- We also may receive information about the device of a non-registered user if that user visits a part of Facebook that does not require people to log in—such as a public Facebook Page. The information we log when people visit our websites or apps is the same as described above and is the same information that any provider of an online service would receive.

- In addition, Facebook may receive some basic information about devices where Facebook apps are installed, including before people using those devices have registered for Facebook (such as when a user downloads a Facebook app, but has not yet created an account, or if the app is preloaded on a given device). This device data includes things like device model, operating system, IP address, app version and device identifiers. We use this information to provide the right version of the app, help people who want to create accounts (for example, optimizing the registration flow for the specific device), retrieving bug fixes and measuring and improving app performance. We do not use this information to build profiles about non-registered users.

443. How do you explain this to your mother?

As discussed with your staff, this question is not germane to the hearing.

444. What will you do with to prevent people from selling false goods on Facebook? I was a victim of that.

We take intellectual property rights seriously at Facebook. Our measures target potential piracy across our products, including Facebook Live, and continue to be enhanced and expanded. These include a global notice-and-takedown program, a comprehensive repeat infringer policy, integration with the content recognition service Audible Magic, and our proprietary video- and audio-matching technology called Rights Manager. More information about these measures can be found in our Intellectual Property Help Center, Transparency Report, and Rights Manager website. Further, Fraudulent ads are not allowed on Facebook. They are in breach of our advertising policies and we will remove them when we find them.

445. My techy husband and I are both flabbergasted at his arrogance and his "I'm above the fray" attitude. Perhaps this can be turned into an appropriate question. Thank you for all you do for us.

As discussed with your staff, this question is not germane to the hearing.

446. Why is it so difficult to delete Facebook pages?

We believe that it's important to communicate with people about the information that we collect and how people can control it. As explained in our Data Policy, we collect three basic categories of data about people:

(1) data about things people do and share (and who they connect with) on our services;

(2) data about the devices people use to access our services; and

(3) data we receive from partners, including the websites and apps that use our business tools.

We collect information about the people, Pages, accounts, hashtags, and groups users are connected to and how they interact with them across our Products, such as people a user communicates with the most or groups users are part of. We also collect contact information if they choose to upload, sync, or import it from a device (such as an address book or call log or SMS log history), which we use for things like helping them and others find people they may know.

The data we use to show ads to people depends on the data we have received from people. For people who are new to Facebook, we may have minimal data that we can use. For people who have used our services for longer, we likely have more data, but the amount of data will depend on the nature of that use and how they have used our controls. Any person can see each of the specific interests we maintain about them for advertising by visiting Ads Preferences, which lets people see what interests we use to choose ads for them—and to edit or delete these

interests. We also provide more detailed information about how we use data to decide what ads to show to people in our "About Facebook Ads" page, at https://www.facebook.com/ads/about. And, we do not sell people's information to anyone, and we never will.

All users must expressly consent to Facebook's Terms and Data Policy when registering for Facebook. The Data Policy explains the kinds of information we collect, how we use this information, how we share this information, and how users can manage and delete information.

Facebook does not create profiles for people without a Facebook account, but we do receive some information from devices and browsers that may be used by non-users. For example:

- When people visit apps or websites that feature our technologies—like the Facebook Like or Comment button—our servers automatically log (i) standard browser or app records of the fact that a particular device or user visited the website or app (this connection to Facebook's servers occurs automatically when a person visits a website or app that contains our technologies, such as a Like button, and is an inherent function of Internet design); and (ii) any additional information the publisher of the app or website chooses to share with Facebook about the person's activities on that site (such as the fact that a purchase was made on the site). This is a standard feature of the Internet, and most websites and apps share this same information with multiple different third-parties whenever people visit their website or app. When the person visiting a website featuring Facebook's tools is not a registered Facebook user, Facebook does not have information identifying that individual, and it does not create profiles for this individual.

- We also may receive information about the device of a non-registered user if that user visits a part of Facebook that does not require people to log in—such as a public Facebook Page. The information we log when people visit our websites or apps is the same as described above and is the same information that any provider of an online service would receive.

- In addition, Facebook may receive some basic information about devices where Facebook apps are installed, including before people using those devices have registered for Facebook (such as when a user downloads a Facebook app, but has not yet created an account, or if the app is preloaded on a given device). This device data includes things like device model, operating system, IP address, app version and device identifiers. We use this information to provide the right version of the app, help people who want to create accounts (for example, optimizing the registration flow for the specific device), retrieving bug fixes and measuring and improving app performance. We do not use this information to build profiles about non-registered users.

447. How's it feel to go from cyber hero to cyber fool in a cyber instant?

As discussed with your staff, this question is not germane to the hearing.

448. Have you considered amongst your options, stepping down and maybe taking a job at Squaw or Heavenly?

We recognize that we have made mistakes, and we are committed to learning from this experience to secure our platform further and make our community safer for everyone going forward. As our CEO Mark Zuckerberg has said, when you are building something unprecedented like Facebook, there are going to be mistakes. What people should hold us accountable for is learning from the mistakes and continually doing better—and, at the end of the day, making sure that we're building things that people like and that make their lives better.

Particularly in the past few months, we've realized that we need to take a broader view of our responsibility to our community. Part of that effort is continuing our ongoing efforts to identify ways that we can improve our privacy practices. We've heard loud and clear that privacy settings and other important tools are too hard to find and that we must do more to keep people informed. So, we're taking additional steps to put people more in control of their privacy. For instance, we redesigned our entire settings menu on mobile devices from top to bottom to make things easier to find. We also created a new Privacy Shortcuts in a menu where users can control their data in just a few taps, with clearer explanations of how our controls work. The experience is now clearer, more visual, and easy-to-find. Furthermore, we also updated our terms of service that include our commitments to everyone using Facebook. We explain the services we offer in language that's easier to read. We've also updated our Data Policy to better spell out what data we collect and how we use it in Facebook, Instagram, Messenger, and other products.

449. Tim Cook, CEO (Apple, Inc.) stated that "privacy is a human right." Do you agree Mr. Zuckerberg?

We believe everyone deserves good privacy controls. A user owns the information they share on Facebook. This means they decide what they share and who they share it with on Facebook, and they can change their mind. We require websites and apps who use our tools to tell users they're collecting and sharing their information with us, and to get users' permission to do so.

Everyone has the right to expect strong protections for their information. We also need to do our part to help keep our community safe, in a way that's consistent with people's privacy expectations. We've recently announced several steps to give people more control over their privacy, including a new Privacy Shortcuts tool that we're rolling out now to give people information about how to control their information, including choosing who can see what they post and adding protections like two-factor authentication to their account. People can learn more about how to protect their privacy in our updated Data Policy and in our Privacy Basics feature (https://www.facebook.com/about/basics).

We are in the process of investigating every app that had access to a large amount of information before we changed our Platform in 2014. The investigation process is in full swing. We have large teams of internal and external experts working hard to investigate these apps as quickly as possible. As of early June 2018, thousands of apps have been investigated and around 200 apps have been suspended—pending a thorough investigation into whether they did in fact misuse any data. Where we find evidence that these or other apps did misuse data, we will ban them and let people know.

Facebook is generally not opposed to regulation but wants to ensure it is the right regulation. The issues facing the industry are complex, multi-faceted, and affect an important part of peoples' lives. As such, Facebook is absolutely committed to working with regulators, like Congress, to craft the right regulations. Facebook would be happy to review any proposed legislation and provide comments.

450. Was all of Mr. Zuckerberg's data accessed? If not why not? Is his data treated differently than a normal users?

We believe that it's important to communicate with people about the information that we collect and how people can control it. As explained in our Data Policy, we collect three basic categories of data about people:

(1) data about things people do and share (and who they connect with) on our services;

(2) data about the devices people use to access our services; and

(3) data we receive from partners, including the websites and apps that use our business tools.

We collect information about the people, Pages, accounts, hashtags, and groups users are connected to and how they interact with them across our Products, such as people a user communicates with the most or groups users are part of. We also collect contact information if they choose to upload, sync, or import it from a device (such as an address book or call log or SMS log history), which we use for things like helping them and others find people they may know.

The data we use to show ads to people depends on the data we have received from people. For people who are new to Facebook, we may have minimal data that we can use. For people who have used our services for longer, we likely have more data, but the amount of data will depend on the nature of that use and how they have used our controls. Any person can see each of the specific interests we maintain about them for advertising by visiting Ads Preferences, which lets people see what interests we use to choose ads for them—and to edit or delete these interests. We also provide more detailed information about how we use data to decide what ads to show to people in our "About Facebook Ads" page, at https://www.facebook.com/ads/about. And, we do not sell people's information to anyone, and we never will.

All users must expressly consent to Facebook's Terms and Data Policy when registering for Facebook. The Data Policy explains the kinds of information we collect, how we use this information, how we share this information, and how users can manage and delete information.

Facebook does not create profiles for people without a Facebook account, but we do receive some information from devices and browsers that may be used by non-users. For example:

- When people visit apps or websites that feature our technologies—like the Facebook Like or Comment button—our servers automatically log (i) standard browser or app records of the fact that a particular device or user visited the website or app (this connection to

Facebook's servers occurs automatically when a person visits a website or app that contains our technologies, such as a Like button, and is an inherent function of Internet design); and (ii) any additional information the publisher of the app or website chooses to share with Facebook about the person's activities on that site (such as the fact that a purchase was made on the site). This is a standard feature of the Internet, and most websites and apps share this same information with multiple different third-parties whenever people visit their website or app. When the person visiting a website featuring Facebook's tools is not a registered Facebook user, Facebook does not have information identifying that individual, and it does not create profiles for this individual.

- We also may receive information about the device of a non-registered user if that user visits a part of Facebook that does not require people to log in—such as a public Facebook Page. The information we log when people visit our websites or apps is the same as described above and is the same information that any provider of an online service would receive.

- In addition, Facebook may receive some basic information about devices where Facebook apps are installed, including before people using those devices have registered for Facebook (such as when a user downloads a Facebook app, but has not yet created an account, or if the app is preloaded on a given device). This device data includes things like device model, operating system, IP address, app version and device identifiers. We use this information to provide the right version of the app, help people who want to create accounts (for example, optimizing the registration flow for the specific device), retrieving bug fixes and measuring and improving app performance. We do not use this information to build profiles about non-registered users.

451. Is your company looking into the next possible threats, beyond data hacking?

For years, we had been aware of other types of activity that appeared to come from Russian sources—largely traditional security threats such as attacking people's accounts or using social media platforms to spread stolen information. What we saw early in the 2016 campaign cycle followed this pattern. Our security team that focuses on threat intelligence—which investigates advanced security threats as part of our overall information security organization—was, from the outset, alert to the possibility of Russian activity. In several instances before November 8, 2016, this team detected and mitigated threats from actors with ties to Russia and reported them to US law enforcement officials. This included activity from a cluster of accounts we had assessed to belong to a group (APT28) that the US government has publicly linked to Russian military intelligence services. This activity, which was aimed at employees of major US political parties, fell into the normal categories of offensive cyber activities we monitor for. We warned the targets who were at highest risk, and were later in contact with law enforcement authorities about this activity.

Later in the summer we also started to see a new kind of behavior from APT28-related accounts—namely, the creation of fake personas that were then used to seed stolen information to journalists. These fake personas were organized under the banner of an organization that called itself DC Leaks. This activity violated our policies, and we removed the DC Leaks accounts.

Facebook learned from press accounts and statements by congressional leaders that Russian actors might have tried to interfere in the 2016 election by exploiting Facebook's ad tools. This is not something we had seen before, and so we started an investigation. We found that fake accounts associated with the IRA tried to influence the election.

This will never be a solved problem because we're up against determined, creative and well-funded adversaries. But we are making steady progress in preventing bad actors from using misinformation to undermine the democratic process, such as: increased ad transparency, advertiser verification and labeling, updating targeting criteria, better technological efforts to find and disable fake accounts, third-party fact checking to stop the spread of false news, doubling the number of people working on safety and security, greater industry collaboration, increased information sharing and reporting channels, proactive identification of election threats, and specific action against the Russia-based IRA.

We will continue to work with the government, and across the tech industry and civil society, to address this important national security matter so that we can do our part to prevent similar abuse from happening again.

452. When are you and Sheryl going to step down and let people with actual ethics run Facebook?

We recognize that we have made mistakes, and we are committed to learning from this experience to secure our platform further and make our community safer for everyone going forward. As our CEO Mark Zuckerberg has said, when you are building something unprecedented like Facebook, there are going to be mistakes. What people should hold us accountable for is learning from the mistakes and continually doing better—and, at the end of the day, making sure that we're building things that people like and that make their lives better.

Particularly in the past few months, we've realized that we need to take a broader view of our responsibility to our community. Part of that effort is continuing our ongoing efforts to identify ways that we can improve our privacy practices. We've heard loud and clear that privacy settings and other important tools are too hard to find and that we must do more to keep people informed. So, we're taking additional steps to put people more in control of their privacy. For instance, we redesigned our entire settings menu on mobile devices from top to bottom to make things easier to find. We also created a new Privacy Shortcuts in a menu where users can control their data in just a few taps, with clearer explanations of how our controls work. The experience is now clearer, more visual, and easy-to-find. Furthermore, we also updated our terms of service that include our commitments to everyone using Facebook. We explain the services we offer in language that's easier to read. We've also updated our Data Policy to better spell out what data we collect and how we use it in Facebook, Instagram, Messenger, and other products.

453. How am I to trust your FB Company in the future?

We believe everyone deserves good privacy controls. A user owns the information they share on Facebook. This means they decide what they share and who they share it with on Facebook, and they can change their mind. We require websites and apps who use our tools to

tell users they're collecting and sharing their information with us, and to get users' permission to do so.

Everyone has the right to expect strong protections for their information. We also need to do our part to help keep our community safe, in a way that's consistent with people's privacy expectations. We've recently announced several steps to give people more control over their privacy, including a new Privacy Shortcuts tool that we're rolling out now to give people information about how to control their information, including choosing who can see what they post and adding protections like two-factor authentication to their account. People can learn more about how to protect their privacy in our updated Data Policy and in our Privacy Basics feature (https://www.facebook.com/about/basics).

We are in the process of investigating every app that had access to a large amount of information before we changed our Platform in 2014. The investigation process is in full swing. We have large teams of internal and external experts working hard to investigate these apps as quickly as possible. As of early June 2018, thousands of apps have been investigated and around 200 apps have been suspended—pending a thorough investigation into whether they did in fact misuse any data. Where we find evidence that these or other apps did misuse data, we will ban them and let people know.

Facebook is generally not opposed to regulation but wants to ensure it is the right regulation. The issues facing the industry are complex, multi-faceted, and affect an important part of peoples' lives. As such, Facebook is absolutely committed to working with regulators, like Congress, to craft the right regulations. Facebook would be happy to review any proposed legislation and provide comments.

454. Does all Technology companies spy on Americans?

We believe that it's important to communicate with people about the information that we collect and how people can control it. As explained in our Data Policy, we collect three basic categories of data about people:

(1) data about things people do and share (and who they connect with) on our services;

(2) data about the devices people use to access our services; and

(3) data we receive from partners, including the websites and apps that use our business tools.

We collect information about the people, Pages, accounts, hashtags, and groups users are connected to and how they interact with them across our Products, such as people a user communicates with the most or groups users are part of. We also collect contact information if they choose to upload, sync, or import it from a device (such as an address book or call log or SMS log history), which we use for things like helping them and others find people they may know.

The data we use to show ads to people depends on the data we have received from people. For people who are new to Facebook, we may have minimal data that we can use. For

people who have used our services for longer, we likely have more data, but the amount of data will depend on the nature of that use and how they have used our controls. Any person can see each of the specific interests we maintain about them for advertising by visiting Ads Preferences, which lets people see what interests we use to choose ads for them—and to edit or delete these interests. We also provide more detailed information about how we use data to decide what ads to show to people in our "About Facebook Ads" page, at https://www.facebook.com/ads/about. And, we do not sell people's information to anyone, and we never will.

All users must expressly consent to Facebook's Terms and Data Policy when registering for Facebook. The Data Policy explains the kinds of information we collect, how we use this information, how we share this information, and how users can manage and delete information.

Facebook does not create profiles for people without a Facebook account, but we do receive some information from devices and browsers that may be used by non-users. For example:

- When people visit apps or websites that feature our technologies—like the Facebook Like or Comment button—our servers automatically log (i) standard browser or app records of the fact that a particular device or user visited the website or app (this connection to Facebook's servers occurs automatically when a person visits a website or app that contains our technologies, such as a Like button, and is an inherent function of Internet design); and (ii) any additional information the publisher of the app or website chooses to share with Facebook about the person's activities on that site (such as the fact that a purchase was made on the site). This is a standard feature of the Internet, and most websites and apps share this same information with multiple different third-parties whenever people visit their website or app. When the person visiting a website featuring Facebook's tools is not a registered Facebook user, Facebook does not have information identifying that individual, and it does not create profiles for this individual.

- We also may receive information about the device of a non-registered user if that user visits a part of Facebook that does not require people to log in—such as a public Facebook Page. The information we log when people visit our websites or apps is the same as described above and is the same information that any provider of an online service would receive.

- In addition, Facebook may receive some basic information about devices where Facebook apps are installed, including before people using those devices have registered for Facebook (such as when a user downloads a Facebook app, but has not yet created an account, or if the app is preloaded on a given device). This device data includes things like device model, operating system, IP address, app version and device identifiers. We use this information to provide the right version of the app, help people who want to create accounts (for example, optimizing the registration flow for the specific device), retrieving bug fixes and measuring and improving app performance. We do not use this information to build profiles about non-registered users.

455. When your executives claim connecting people at any cost is good, how do you hold them accountable?

We recognize that we have made mistakes, and we are committed to learning from this experience to secure our platform further and make our community safer for everyone going forward. As our CEO Mark Zuckerberg has said, when you are building something unprecedented like Facebook, there are going to be mistakes. What people should hold us accountable for is learning from the mistakes and continually doing better—and, at the end of the day, making sure that we're building things that people like and that make their lives better.

Particularly in the past few months, we've realized that we need to take a broader view of our responsibility to our community. Part of that effort is continuing our ongoing efforts to identify ways that we can improve our privacy practices. We've heard loud and clear that privacy settings and other important tools are too hard to find and that we must do more to keep people informed. So, we're taking additional steps to put people more in control of their privacy. For instance, we redesigned our entire settings menu on mobile devices from top to bottom to make things easier to find. We also created a new Privacy Shortcuts in a menu where users can control their data in just a few taps, with clearer explanations of how our controls work. The experience is now clearer, more visual, and easy-to-find. Furthermore, we also updated our terms of service that include our commitments to everyone using Facebook. We explain the services we offer in language that's easier to read. We've also updated our Data Policy to better spell out what data we collect and how we use it in Facebook, Instagram, Messenger, and other products.

456. What is the Facebook's internal Mission Statement and how do Corporate Officers measure your progress?

We recognize that we have made mistakes, and we are committed to learning from this experience to secure our platform further and make our community safer for everyone going forward. As our CEO Mark Zuckerberg has said, when you are building something unprecedented like Facebook, there are going to be mistakes. What people should hold us accountable for is learning from the mistakes and continually doing better—and, at the end of the day, making sure that we're building things that people like and that make their lives better.

Particularly in the past few months, we've realized that we need to take a broader view of our responsibility to our community. Part of that effort is continuing our ongoing efforts to identify ways that we can improve our privacy practices. We've heard loud and clear that privacy settings and other important tools are too hard to find and that we must do more to keep people informed. So, we're taking additional steps to put people more in control of their privacy. For instance, we redesigned our entire settings menu on mobile devices from top to bottom to make things easier to find. We also created a new Privacy Shortcuts in a menu where users can control their data in just a few taps, with clearer explanations of how our controls work. The experience is now clearer, more visual, and easy-to-find. Furthermore, we also updated our terms of service that include our commitments to everyone using Facebook. We explain the services we offer in language that's easier to read. We've also updated our Data Policy to better spell out what data we collect and how we use it in Facebook, Instagram, Messenger, and other products.

457. How many privacy analysts does Facebook employ?

We believe everyone deserves good privacy controls. A user owns the information they share on Facebook. This means they decide what they share and who they share it with on

Facebook, and they can change their mind. We require websites and apps who use our tools to tell users they're collecting and sharing their information with us, and to get users' permission to do so.

Everyone has the right to expect strong protections for their information. We also need to do our part to help keep our community safe, in a way that's consistent with people's privacy expectations. We've recently announced several steps to give people more control over their privacy, including a new Privacy Shortcuts tool that we're rolling out now to give people information about how to control their information, including choosing who can see what they post and adding protections like two-factor authentication to their account. People can learn more about how to protect their privacy in our updated Data Policy and in our Privacy Basics feature (https://www.facebook.com/about/basics).

We are in the process of investigating every app that had access to a large amount of information before we changed our Platform in 2014. The investigation process is in full swing. We have large teams of internal and external experts working hard to investigate these apps as quickly as possible. As of early June 2018, thousands of apps have been investigated and around 200 apps have been suspended—pending a thorough investigation into whether they did in fact misuse any data. Where we find evidence that these or other apps did misuse data, we will ban them and let people know.

Facebook is generally not opposed to regulation but wants to ensure it is the right regulation. The issues facing the industry are complex, multi-faceted, and affect an important part of peoples' lives. As such, Facebook is absolutely committed to working with regulators, like Congress, to craft the right regulations. Facebook would be happy to review any proposed legislation and provide comments.

458. Given this critical breach of public trust, does the current leadership of Facebook need to be replaced?

We recognize that we have made mistakes, and we are committed to learning from this experience to secure our platform further and make our community safer for everyone going forward. As our CEO Mark Zuckerberg has said, when you are building something unprecedented like Facebook, there are going to be mistakes. What people should hold us accountable for is learning from the mistakes and continually doing better—and, at the end of the day, making sure that we're building things that people like and that make their lives better.

Particularly in the past few months, we've realized that we need to take a broader view of our responsibility to our community. Part of that effort is continuing our ongoing efforts to identify ways that we can improve our privacy practices. We've heard loud and clear that privacy settings and other important tools are too hard to find and that we must do more to keep people informed. So, we're taking additional steps to put people more in control of their privacy. For instance, we redesigned our entire settings menu on mobile devices from top to bottom to make things easier to find. We also created a new Privacy Shortcuts in a menu where users can control their data in just a few taps, with clearer explanations of how our controls work. The experience is now clearer, more visual, and easy-to-find. Furthermore, we also updated our terms of service that include our commitments to everyone using Facebook. We explain the services we offer in

language that's easier to read. We've also updated our Data Policy to better spell out what data we collect and how we use it in Facebook, Instagram, Messenger, and other products.

459. Did you profit from your mistake?

We believe that it's important to communicate with people about the information that we collect and how people can control it. As explained in our Data Policy, we collect three basic categories of data about people:

(1) data about things people do and share (and who they connect with) on our services;

(2) data about the devices people use to access our services; and

(3) data we receive from partners, including the websites and apps that use our business tools.

We collect information about the people, Pages, accounts, hashtags, and groups users are connected to and how they interact with them across our Products, such as people a user communicates with the most or groups users are part of. We also collect contact information if they choose to upload, sync, or import it from a device (such as an address book or call log or SMS log history), which we use for things like helping them and others find people they may know.

The data we use to show ads to people depends on the data we have received from people. For people who are new to Facebook, we may have minimal data that we can use. For people who have used our services for longer, we likely have more data, but the amount of data will depend on the nature of that use and how they have used our controls. Any person can see each of the specific interests we maintain about them for advertising by visiting Ads Preferences, which lets people see what interests we use to choose ads for them—and to edit or delete these interests. We also provide more detailed information about how we use data to decide what ads to show to people in our "About Facebook Ads" page, at https://www.facebook.com/ads/about. And, we do not sell people's information to anyone, and we never will.

All users must expressly consent to Facebook's Terms and Data Policy when registering for Facebook. The Data Policy explains the kinds of information we collect, how we use this information, how we share this information, and how users can manage and delete information.

Facebook does not create profiles for people without a Facebook account, but we do receive some information from devices and browsers that may be used by non-users. For example:

- When people visit apps or websites that feature our technologies—like the Facebook Like or Comment button—our servers automatically log (i) standard browser or app records of the fact that a particular device or user visited the website or app (this connection to Facebook's servers occurs automatically when a person visits a website or app that contains our technologies, such as a Like button, and is an inherent function of Internet design); and (ii) any additional information the publisher of the app or website chooses to share with Facebook about the person's activities on that site (such as the fact that a

purchase was made on the site). This is a standard feature of the Internet, and most websites and apps share this same information with multiple different third-parties whenever people visit their website or app. When the person visiting a website featuring Facebook's tools is not a registered Facebook user, Facebook does not have information identifying that individual, and it does not create profiles for this individual.

- We also may receive information about the device of a non-registered user if that user visits a part of Facebook that does not require people to log in—such as a public Facebook Page. The information we log when people visit our websites or apps is the same as described above and is the same information that any provider of an online service would receive.

- In addition, Facebook may receive some basic information about devices where Facebook apps are installed, including before people using those devices have registered for Facebook (such as when a user downloads a Facebook app, but has not yet created an account, or if the app is preloaded on a given device). This device data includes things like device model, operating system, IP address, app version and device identifiers. We use this information to provide the right version of the app, help people who want to create accounts (for example, optimizing the registration flow for the specific device), retrieving bug fixes and measuring and improving app performance. We do not use this information to build profiles about non-registered users.

460. What does Facebook plan to do to leverage its platform to facilitate a desirable future for all?

We want our platform to be a place where people can have authentic conversations about elections and other political topics. We believe this kind of engagement promotes democracy, but we know that there are actors working to interfere with those conversations and undermine our elections. We are already taking steps to proactively prevent election interference and we are strengthening these protections going forward.

Engagement with campaigns: We want all candidates, groups, and voters to use our platform to engage in elections. We want it to be easy for people to find, follow, and contact their elected representatives—and those running to represent them. That's why, for candidates across the political spectrum, Facebook offers the same levels of support in key moments to help campaigns understand how best to use the platform. Both the Obama and Romney campaigns had access to the same tools, and no campaign received any special treatment from Facebook. Likewise, we offered identical support to both the Trump and Clinton campaigns, and had teams assigned to both. Everyone had access to the same tools, which are the same tools that every campaign is offered, and is consistent with support provided to commercial clients in the normal course of business. Facebook representatives advise political advertisers on Facebook, as they would with other, non-political managed accounts. We have a compliance team that trains our sales representatives to comply with all federal election law requirements in this area.

While no one from Facebook was assigned full-time to the Trump campaign, Facebook employees did interact with Cambridge Analytica employees. While our investigation is ongoing, our review indicates that Facebook employees did not identify any issues involving the

improper use of Facebook data in the course of their interactions with Cambridge Analytica during the 2016 US Presidential campaign.

Election Integrity: In the run-up to the 2016 elections, we were focused on the kinds of cybersecurity attacks typically used by nation states, for example phishing and malware attacks. And we were too slow to spot information operations interference. Since then, we've made important changes to prevent bad actors from using misinformation to undermine the democratic process. This will never be a solved problem because we're up against determined, creative and well-funded adversaries. But we are making steady progress. Here is a list of the 10 most important changes we have made:

- **Ads transparency.** Advertising should be transparent: users should be able to see all the ads an advertiser is currently running on Facebook, Instagram and Messenger. And for ads with political content, we've created an archive that will hold ads with political content for seven years—including information about ad impressions and spend, as well as demographic data such as age, gender and location. People in Canada and Ireland have already been able to see all the ads that a Page is running on Facebook—and we've launched this globally.

- **Verification and labeling.** Every advertiser will now need to confirm their ID and location before being able to run any ads with political content in the US. All ads with political content will also clearly state who paid for them.

- **Updating targeting.** We want ads on Facebook to be safe and civil. We thoroughly review the targeting criteria advertisers can use to ensure they are consistent with our principles. As a result, we removed nearly one-third of the targeting segments used by the IRA. We continue to allow some criteria that people may find controversial. But we do see businesses marketing things like historical books, documentaries or television shows using them in legitimate ways.

- **Better technology.** Over the past year, we've gotten increasingly better at finding and disabling fake accounts. We now block millions of fake accounts each day as people try to create them—and before they've done any harm. This is thanks to improvements in machine learning and artificial intelligence, which can proactively identify suspicious behavior at a scale that was not possible before—without needing to look at the content itself.

- **Action to tackle fake news.** We are working hard to stop the spread of false news. We work with third-party fact-checking organizations to limit the spread of articles rated false. To reduce the spread of false news, we remove fake accounts and disrupt economic incentives for traffickers of misinformation. We also use various signals, including feedback from our community, to identify potential false news. In countries where we have partnerships with independent third-party fact-checkers, stories rated as false by those fact-checkers are shown lower in News Feed. If Pages or domains repeatedly create or share misinformation, we significantly reduce their distribution and remove their advertising rights. We also want to empower people to decide for themselves what to read, trust, and share. We promote news literacy and work to inform people with more

context. For example, if third-party fact-checkers write articles about a news story, we show them immediately below the story in the Related Articles unit. We also notify people and Page Admins if they try to share a story, or have shared one in the past, that's been determined to be false. In addition to our own efforts, we're learning from academics, scaling our partnerships with third-party fact-checkers and talking to other organizations about how we can work together.

A key focus is working to disrupt the economics of fake news. For example, preventing the creation of fake accounts that spread it, banning sites that engage in this behavior from using our ad products, and demoting articles found to be false by fact checkers in News Feed—causing it to lose 80% of its traffic. We now work with independent fact checkers in the US, France, Germany, Ireland, the Netherlands, Italy, Mexico, Colombia, India, Indonesia and the Philippines with plans to scale to more countries in the coming months.

- **Significant investments in security.** We're doubling the number of people working on safety and security from 10,000 last year to over 20,000 this year. We expect these investments to impact our profitability. But the safety of people using Facebook needs to come before profit.

- **Industry collaboration.** Recently, we joined 34 global tech and security companies in signing a TechAccord pact to help improve security for everyone.

- **Information sharing and reporting channels.** In the 2017 German elections, we worked closely with the authorities there, including the Federal Office for Information Security (BSI). This gave them a dedicated reporting channel for security issues related to the federal elections.

- **Tracking 40+ elections.** In recent months, we've started to deploy new tools and teams to proactively identify threats in the run-up to specific elections. We first tested this effort during the Alabama Senate election, and plan to continue these efforts for elections around the globe, including the US midterms. Last year we used public service announcements to help inform people about fake news in 21 separate countries, including in advance of French, Kenyan and German elections.

- **Action against the Russia-based IRA.** In April, we removed 70 Facebook and 65 Instagram accounts—as well as 138 Facebook Pages—controlled by the IRA primarily targeted either at people living in Russia or Russian-speakers around the world including from neighboring countries like Azerbaijan, Uzbekistan and Ukraine. The IRA has repeatedly used complex networks of inauthentic accounts to deceive and manipulate people in the US, Europe and Russia—and we don't want them on Facebook anywhere in the world.

461. What are the fines, penalties for Facebook's violating its 2011 deal to better protect its users? Stop pussy-footing around these tech giants. Thank you for this opportunity. Florence

Protecting people's data is one of our most important responsibilities, and we are committed to continuing our work to improve how we protect people's information and to working with regulators to draft appropriate regulations. Our mission is to give people the power to build community and bring the world closer together. As the internet becomes more important in people's lives, the real question is about the right set of regulations that should apply to all internet services, regardless of size. Across the board, we have a responsibility to not just build tools, but to make sure that they're used in ways that are positive for our users. Facebook is generally not opposed to regulation but wants to ensure it is the right regulation. The issues facing the industry are complex, multi-faceted, and affect an important part of peoples' lives. As such, Facebook is absolutely committed to working with regulators, like Congress, to craft the right regulations.

We are already regulated in many ways—for example, under the Federal Trade Commission Act—and we are subject to ongoing oversight by the FTC under the terms of a 2011 consent order. We furnished extensive information to the FTC regarding the ability for users to port their Facebook data (including friends data that had been shared with them) with apps on Facebook's platform, as part of the FTC's investigation culminating in the July 27, 2012 Consent Order. The Consent Order memorializes the agreement between Facebook and the FTC and did not require Facebook to turn off or change the ability for people to port friends data that had been shared with them on Facebook to apps they used. Facebook voluntarily changed this feature of Platform in 2014, however. Facebook has not violated the Federal Trade Commission Act. Facebook is not in a position to determine whether third-party app developers violated the Act and leaves that determination to the FTC, although we can confirm that misrepresenting the terms of an app to users is a violation of Facebook's developer policies.

Facebook has inherent incentives to protect its customers' privacy and address breaches and vulnerabilities. Indeed, the recent discovery of misconduct by an app developer on the Facebook platform clearly hurt Facebook and made it harder for us to achieve our social mission. As such, Facebook is committed to protecting our platform from bad actors, ensuring we are able to continue our mission of giving people a voice and bringing them closer together. It will take some time to work through all the changes we need to make across the company, but Facebook is committed to getting this right.

462. This country supports free enterprise, but not monopolies. What prevents FAANG from becoming a Mon?

Protecting people's data is one of our most important responsibilities, and we are committed to continuing our work to improve how we protect people's information and to working with regulators to draft appropriate regulations. Our mission is to give people the power to build community and bring the world closer together. As the internet becomes more important in people's lives, the real question is about the right set of regulations that should apply to all internet services, regardless of size. Across the board, we have a responsibility to not just build tools, but to make sure that they're used in ways that are positive for our users. Facebook is generally not opposed to regulation but wants to ensure it is the right regulation. The issues facing the industry are complex, multi-faceted, and affect an important part of peoples' lives. As such, Facebook is absolutely committed to working with regulators, like Congress, to craft the right regulations.

We are already regulated in many ways—for example, under the Federal Trade Commission Act—and we are subject to ongoing oversight by the FTC under the terms of a 2011 consent order. We furnished extensive information to the FTC regarding the ability for users to port their Facebook data (including friends data that had been shared with them) with apps on Facebook's platform, as part of the FTC's investigation culminating in the July 27, 2012 Consent Order. The Consent Order memorializes the agreement between Facebook and the FTC and did not require Facebook to turn off or change the ability for people to port friends data that had been shared with them on Facebook to apps they used. Facebook voluntarily changed this feature of Platform in 2014, however. Facebook has not violated the Federal Trade Commission Act. Facebook is not in a position to determine whether third-party app developers violated the Act and leaves that determination to the FTC, although we can confirm that misrepresenting the terms of an app to users is a violation of Facebook's developer policies.

Facebook has inherent incentives to protect its customers' privacy and address breaches and vulnerabilities. Indeed, the recent discovery of misconduct by an app developer on the Facebook platform clearly hurt Facebook and made it harder for us to achieve our social mission. As such, Facebook is committed to protecting our platform from bad actors, ensuring we are able to continue our mission of giving people a voice and bringing them closer together. It will take some time to work through all the changes we need to make across the company, but Facebook is committed to getting this right.

463. I'm now getting Facebook communiques from real estate agents for my house which isn't in the market, a) Is there a 'privacy' button which can filter out unwanted spam? And b) suggestion: have source-identifier attribute to messages.

We believe that it's important to communicate with people about the information that we collect and how people can control it. As explained in our Data Policy, we collect three basic categories of data about people:

(1) data about things people do and share (and who they connect with) on our services;

(2) data about the devices people use to access our services; and

(3) data we receive from partners, including the websites and apps that use our business tools.

We collect information about the people, Pages, accounts, hashtags, and groups users are connected to and how they interact with them across our Products, such as people a user communicates with the most or groups users are part of. We also collect contact information if they choose to upload, sync, or import it from a device (such as an address book or call log or SMS log history), which we use for things like helping them and others find people they may know.

The data we use to show ads to people depends on the data we have received from people. For people who are new to Facebook, we may have minimal data that we can use. For people who have used our services for longer, we likely have more data, but the amount of data will depend on the nature of that use and how they have used our controls. Any person can see each of the specific interests we maintain about them for advertising by visiting Ads Preferences,

which lets people see what interests we use to choose ads for them—and to edit or delete these interests. We also provide more detailed information about how we use data to decide what ads to show to people in our "About Facebook Ads" page, at https://www.facebook.com/ads/about. And, we do not sell people's information to anyone, and we never will.

All users must expressly consent to Facebook's Terms and Data Policy when registering for Facebook. The Data Policy explains the kinds of information we collect, how we use this information, how we share this information, and how users can manage and delete information.

Facebook does not create profiles for people without a Facebook account, but we do receive some information from devices and browsers that may be used by non-users. For example:

- When people visit apps or websites that feature our technologies—like the Facebook Like or Comment button—our servers automatically log (i) standard browser or app records of the fact that a particular device or user visited the website or app (this connection to Facebook's servers occurs automatically when a person visits a website or app that contains our technologies, such as a Like button, and is an inherent function of Internet design); and (ii) any additional information the publisher of the app or website chooses to share with Facebook about the person's activities on that site (such as the fact that a purchase was made on the site). This is a standard feature of the Internet, and most websites and apps share this same information with multiple different third-parties whenever people visit their website or app. When the person visiting a website featuring Facebook's tools is not a registered Facebook user, Facebook does not have information identifying that individual, and it does not create profiles for this individual.

- We also may receive information about the device of a non-registered user if that user visits a part of Facebook that does not require people to log in—such as a public Facebook Page. The information we log when people visit our websites or apps is the same as described above and is the same information that any provider of an online service would receive.

- In addition, Facebook may receive some basic information about devices where Facebook apps are installed, including before people using those devices have registered for Facebook (such as when a user downloads a Facebook app, but has not yet created an account, or if the app is preloaded on a given device). This device data includes things like device model, operating system, IP address, app version and device identifiers. We use this information to provide the right version of the app, help people who want to create accounts (for example, optimizing the registration flow for the specific device), retrieving bug fixes and measuring and improving app performance. We do not use this information to build profiles about non-registered users.

464. In his opinion, should we be worried about the practices of other social media?

We believe everyone deserves good privacy controls. A user owns the information they share on Facebook. This means they decide what they share and who they share it with on Facebook, and they can change their mind. We require websites and apps who use our tools to

tell users they're collecting and sharing their information with us, and to get users' permission to do so.

Everyone has the right to expect strong protections for their information. We also need to do our part to help keep our community safe, in a way that's consistent with people's privacy expectations. We've recently announced several steps to give people more control over their privacy, including a new Privacy Shortcuts tool that we're rolling out now to give people information about how to control their information, including choosing who can see what they post and adding protections like two-factor authentication to their account. People can learn more about how to protect their privacy in our updated Data Policy and in our Privacy Basics feature (https://www.facebook.com/about/basics).

We are in the process of investigating every app that had access to a large amount of information before we changed our Platform in 2014. The investigation process is in full swing. We have large teams of internal and external experts working hard to investigate these apps as quickly as possible. As of early June 2018, thousands of apps have been investigated and around 200 apps have been suspended—pending a thorough investigation into whether they did in fact misuse any data. Where we find evidence that these or other apps did misuse data, we will ban them and let people know.

Facebook is generally not opposed to regulation but wants to ensure it is the right regulation. The issues facing the industry are complex, multi-faceted, and affect an important part of peoples' lives. As such, Facebook is absolutely committed to working with regulators, like Congress, to craft the right regulations. Facebook would be happy to review any proposed legislation and provide comments.

465. There is no justification for putting profit before privacy.

As discussed with your staff, this question is not germane to the hearing.

466. How do users know if their data has been compromised? Can you ensure faster response time if this happens in the future?

Facebook's policies regarding third-party usage of its platform technologies have prohibited—and continue to prohibit—third-party app developers from selling or licensing user data accessed from Facebook and from sharing any user data accessed from Facebook with any ad network, data broker or other advertising or monetization-related service. We take action on potential violations of our Platform Policies based on proactive review, external reports, and other signals. Kogan was not permitted to sell or transfer data to third-parties for the purposes he did. In doing so, Kogan and his company violated Facebook's Platform Policies.

On December 11, 2015, *The Guardian* published an article reporting that Kogan and his company, GSR, may have passed information the app had obtained from Facebook users to SCL Elections Ltd. (SCL)/Cambridge Analytica. Facebook immediately banned Kogan's app from our platform and investigated what happened and what further action Facebook should take to enforce our Platform Policies. Facebook considered the matter closed after obtaining written certifications and confirmations from Kogan, GSR, Cambridge Analytica, and SCL declaring that all such data they had obtained was accounted for and destroyed. We did not have any

reason to affirmatively question the veracity of any of these certifications until March 2018, when we learned from media reporting that questions had been raised concerning the accuracy of the certifications. Facebook immediately banned Cambridge Analytica and SCL from purchasing advertisements on our services as well as removed the personal accounts of some of their officers. Moreover, while Facebook's policies in place at the time allowed us to audit apps to ensure that they were safe and did not violate its terms, we had already terminated Kogan's app's access to Facebook. Accordingly, there were no ongoing concerns about the level of data that app could access or might access in the future. With the benefit of hindsight, we wish we had notified people whose information may have been impacted. Facebook has since notified all people potentially impacted with a detailed notice at the top of their News Feed.

467. Why can you delete your Facebook data permanently but users cannot?

We believe that it's important to communicate with people about the information that we collect and how people can control it. As explained in our Data Policy, we collect three basic categories of data about people:

(1) data about things people do and share (and who they connect with) on our services;

(2) data about the devices people use to access our services; and

(3) data we receive from partners, including the websites and apps that use our business tools.

We collect information about the people, Pages, accounts, hashtags, and groups users are connected to and how they interact with them across our Products, such as people a user communicates with the most or groups users are part of. We also collect contact information if they choose to upload, sync, or import it from a device (such as an address book or call log or SMS log history), which we use for things like helping them and others find people they may know.

The data we use to show ads to people depends on the data we have received from people. For people who are new to Facebook, we may have minimal data that we can use. For people who have used our services for longer, we likely have more data, but the amount of data will depend on the nature of that use and how they have used our controls. Any person can see each of the specific interests we maintain about them for advertising by visiting Ads Preferences, which lets people see what interests we use to choose ads for them—and to edit or delete these interests. We also provide more detailed information about how we use data to decide what ads to show to people in our "About Facebook Ads" page, at https://www.facebook.com/ads/about. And, we do not sell people's information to anyone, and we never will.

All users must expressly consent to Facebook's Terms and Data Policy when registering for Facebook. The Data Policy explains the kinds of information we collect, how we use this information, how we share this information, and how users can manage and delete information.

Facebook does not create profiles for people without a Facebook account, but we do receive some information from devices and browsers that may be used by non-users. For example:

- When people visit apps or websites that feature our technologies—like the Facebook Like or Comment button—our servers automatically log (i) standard browser or app records of the fact that a particular device or user visited the website or app (this connection to Facebook's servers occurs automatically when a person visits a website or app that contains our technologies, such as a Like button, and is an inherent function of Internet design); and (ii) any additional information the publisher of the app or website chooses to share with Facebook about the person's activities on that site (such as the fact that a purchase was made on the site). This is a standard feature of the Internet, and most websites and apps share this same information with multiple different third-parties whenever people visit their website or app. When the person visiting a website featuring Facebook's tools is not a registered Facebook user, Facebook does not have information identifying that individual, and it does not create profiles for this individual.

- We also may receive information about the device of a non-registered user if that user visits a part of Facebook that does not require people to log in—such as a public Facebook Page. The information we log when people visit our websites or apps is the same as described above and is the same information that any provider of an online service would receive.

- In addition, Facebook may receive some basic information about devices where Facebook apps are installed, including before people using those devices have registered for Facebook (such as when a user downloads a Facebook app, but has not yet created an account, or if the app is preloaded on a given device). This device data includes things like device model, operating system, IP address, app version and device identifiers. We use this information to provide the right version of the app, help people who want to create accounts (for example, optimizing the registration flow for the specific device), retrieving bug fixes and measuring and improving app performance. We do not use this information to build profiles about non-registered users.

468. Facebook made promises in 2010-11 to protect users. It did not. Now?

Protecting people's data is one of our most important responsibilities, and we are committed to continuing our work to improve how we protect people's information and to working with regulators to draft appropriate regulations. Our mission is to give people the power to build community and bring the world closer together. As the internet becomes more important in people's lives, the real question is about the right set of regulations that should apply to all internet services, regardless of size. Across the board, we have a responsibility to not just build tools, but to make sure that they're used in ways that are positive for our users. Facebook is generally not opposed to regulation but wants to ensure it is the right regulation. The issues facing the industry are complex, multi-faceted, and affect an important part of peoples' lives. As such, Facebook is absolutely committed to working with regulators, like Congress, to craft the right regulations.

We are already regulated in many ways—for example, under the Federal Trade Commission Act—and we are subject to ongoing oversight by the FTC under the terms of a 2011 consent order. We furnished extensive information to the FTC regarding the ability for users to port their Facebook data (including friends data that had been shared with them) with apps on

Facebook's platform, as part of the FTC's investigation culminating in the July 27, 2012 Consent Order. The Consent Order memorializes the agreement between Facebook and the FTC and did not require Facebook to turn off or change the ability for people to port friends data that had been shared with them on Facebook to apps they used. Facebook voluntarily changed this feature of Platform in 2014, however. Facebook has not violated the Federal Trade Commission Act. Facebook is not in a position to determine whether third-party app developers violated the Act and leaves that determination to the FTC, although we can confirm that misrepresenting the terms of an app to users is a violation of Facebook's developer policies.

Facebook has inherent incentives to protect its customers' privacy and address breaches and vulnerabilities. Indeed, the recent discovery of misconduct by an app developer on the Facebook platform clearly hurt Facebook and made it harder for us to achieve our social mission. As such, Facebook is committed to protecting our platform from bad actors, ensuring we are able to continue our mission of giving people a voice and bringing them closer together. It will take some time to work through all the changes we need to make across the company, but Facebook is committed to getting this right.

469. Why would you put your personal wealth ahead of the interests of the citizens and future of the U.S.?

As discussed with your staff, this question is not germane to the hearing.

470. As a social MEDIA company, why do they not comply with media advertising rules?

To build a secure product with extensive infrastructure that connects people wherever they live or whatever their income level, we need to make sure everyone can afford it. Advertising lets us keep Facebook free, which ensures it remains affordable for everyone. We also believe the ads you see across the Facebook family of apps and services should be useful and relevant to you. Users can't opt out of seeing ads altogether because selling ads is what keeps Facebook free, but they do have different options to control how their data can and can't be used to show them ads. They're all found in ad preferences, which allows users to turn off the use of all data collected from partners off Facebook to target ads. Users can also decide which of their profile fields they want used for ad targeting in the Information section under "About you." Users can remove themselves from interests under "Your interests" and categories under "Your categories." And, we do not sell people's information to anyone, and we never will.

Facebook is committed to transparency for all ads, including ads with political content. Facebook believes that people should be able to easily understand why they are seeing ads, who paid for them, and what other ads those advertisers are running. As such, Facebook only allows authorized advertisers to run ads about elections or issues that are being debated across the country. In order to be authorized by Facebook, advertisers will need to confirm their identity and location. Furthermore, all political and issue ads will include a disclosure which reads: "Paid for by," and when users click on this disclosure they will be able to see details about the advertiser. Users will also be able to see an explanation of why they saw the particular ad. This is similar to the disclosure included on political TV advertisements. We just launched globally View Active Ads, a feature that will enable anyone to see all of the ads an advertiser is currently running by visiting the advertiser's Facebook Page.

471. Why are people unable to delete their accounts?

We believe that it's important to communicate with people about the information that we collect and how people can control it. As explained in our Data Policy, we collect three basic categories of data about people:

(1) data about things people do and share (and who they connect with) on our services;

(2) data about the devices people use to access our services; and

(3) data we receive from partners, including the websites and apps that use our business tools.

We collect information about the people, Pages, accounts, hashtags, and groups users are connected to and how they interact with them across our Products, such as people a user communicates with the most or groups users are part of. We also collect contact information if they choose to upload, sync, or import it from a device (such as an address book or call log or SMS log history), which we use for things like helping them and others find people they may know.

The data we use to show ads to people depends on the data we have received from people. For people who are new to Facebook, we may have minimal data that we can use. For people who have used our services for longer, we likely have more data, but the amount of data will depend on the nature of that use and how they have used our controls. Any person can see each of the specific interests we maintain about them for advertising by visiting Ads Preferences, which lets people see what interests we use to choose ads for them—and to edit or delete these interests. We also provide more detailed information about how we use data to decide what ads to show to people in our "About Facebook Ads" page, at https://www.facebook.com/ads/about. And, we do not sell people's information to anyone, and we never will.

All users must expressly consent to Facebook's Terms and Data Policy when registering for Facebook. The Data Policy explains the kinds of information we collect, how we use this information, how we share this information, and how users can manage and delete information.

Facebook does not create profiles for people without a Facebook account, but we do receive some information from devices and browsers that may be used by non-users. For example:

- When people visit apps or websites that feature our technologies—like the Facebook Like or Comment button—our servers automatically log (i) standard browser or app records of the fact that a particular device or user visited the website or app (this connection to Facebook's servers occurs automatically when a person visits a website or app that contains our technologies, such as a Like button, and is an inherent function of Internet design); and (ii) any additional information the publisher of the app or website chooses to share with Facebook about the person's activities on that site (such as the fact that a purchase was made on the site). This is a standard feature of the Internet, and most websites and apps share this same information with multiple different third-parties whenever people visit their website or app. When the person visiting a website featuring

Facebook's tools is not a registered Facebook user, Facebook does not have information identifying that individual, and it does not create profiles for this individual.

- We also may receive information about the device of a non-registered user if that user visits a part of Facebook that does not require people to log in—such as a public Facebook Page. The information we log when people visit our websites or apps is the same as described above and is the same information that any provider of an online service would receive.

- In addition, Facebook may receive some basic information about devices where Facebook apps are installed, including before people using those devices have registered for Facebook (such as when a user downloads a Facebook app, but has not yet created an account, or if the app is preloaded on a given device). This device data includes things like device model, operating system, IP address, app version and device identifiers. We use this information to provide the right version of the app, help people who want to create accounts (for example, optimizing the registration flow for the specific device), retrieving bug fixes and measuring and improving app performance. We do not use this information to build profiles about non-registered users.

472. FB users have few alternatives if they leave; is this as an opportunity to serve or to exploit?

Protecting people's data is one of our most important responsibilities, and we are committed to continuing our work to improve how we protect people's information and to working with regulators to draft appropriate regulations. Our mission is to give people the power to build community and bring the world closer together. As the internet becomes more important in people's lives, the real question is about the right set of regulations that should apply to all internet services, regardless of size. Across the board, we have a responsibility to not just build tools, but to make sure that they're used in ways that are positive for our users. Facebook is generally not opposed to regulation but wants to ensure it is the right regulation. The issues facing the industry are complex, multi-faceted, and affect an important part of peoples' lives. As such, Facebook is absolutely committed to working with regulators, like Congress, to craft the right regulations.

We are already regulated in many ways—for example, under the Federal Trade Commission Act—and we are subject to ongoing oversight by the FTC under the terms of a 2011 consent order. We furnished extensive information to the FTC regarding the ability for users to port their Facebook data (including friends data that had been shared with them) with apps on Facebook's platform, as part of the FTC's investigation culminating in the July 27, 2012 Consent Order. The Consent Order memorializes the agreement between Facebook and the FTC and did not require Facebook to turn off or change the ability for people to port friends data that had been shared with them on Facebook to apps they used. Facebook voluntarily changed this feature of Platform in 2014, however. Facebook has not violated the Federal Trade Commission Act. Facebook is not in a position to determine whether third-party app developers violated the Act and leaves that determination to the FTC, although we can confirm that misrepresenting the terms of an app to users is a violation of Facebook's developer policies.

Facebook has inherent incentives to protect its customers' privacy and address breaches and vulnerabilities. Indeed, the recent discovery of misconduct by an app developer on the Facebook platform clearly hurt Facebook and made it harder for us to achieve our social mission. As such, Facebook is committed to protecting our platform from bad actors, ensuring we are able to continue our mission of giving people a voice and bringing them closer together. It will take some time to work through all the changes we need to make across the company, but Facebook is committed to getting this right.

473. Given what has happened, setting aside what you say FB will do in the future, why should the American public trust you?

We believe everyone deserves good privacy controls. A user owns the information they share on Facebook. This means they decide what they share and who they share it with on Facebook, and they can change their mind. We require websites and apps who use our tools to tell users they're collecting and sharing their information with us, and to get users' permission to do so.

Everyone has the right to expect strong protections for their information. We also need to do our part to help keep our community safe, in a way that's consistent with people's privacy expectations. We've recently announced several steps to give people more control over their privacy, including a new Privacy Shortcuts tool that we're rolling out now to give people information about how to control their information, including choosing who can see what they post and adding protections like two-factor authentication to their account. People can learn more about how to protect their privacy in our updated Data Policy and in our Privacy Basics feature (https://www.facebook.com/about/basics).

We are in the process of investigating every app that had access to a large amount of information before we changed our Platform in 2014. The investigation process is in full swing. We have large teams of internal and external experts working hard to investigate these apps as quickly as possible. As of early June 2018, thousands of apps have been investigated and around 200 apps have been suspended—pending a thorough investigation into whether they did in fact misuse any data. Where we find evidence that these or other apps did misuse data, we will ban them and let people know.

Facebook is generally not opposed to regulation but wants to ensure it is the right regulation. The issues facing the industry are complex, multi-faceted, and affect an important part of peoples' lives. As such, Facebook is absolutely committed to working with regulators, like Congress, to craft the right regulations. Facebook would be happy to review any proposed legislation and provide comments.

474. When will Facebook provide its users the capability to completely erase their content and history?

We believe that it's important to communicate with people about the information that we collect and how people can control it. As explained in our Data Policy, we collect three basic categories of data about people:

(1) data about things people do and share (and who they connect with) on our services;

(2) data about the devices people use to access our services; and

(3) data we receive from partners, including the websites and apps that use our business tools.

We collect information about the people, Pages, accounts, hashtags, and groups users are connected to and how they interact with them across our Products, such as people a user communicates with the most or groups users are part of. We also collect contact information if they choose to upload, sync, or import it from a device (such as an address book or call log or SMS log history), which we use for things like helping them and others find people they may know.

The data we use to show ads to people depends on the data we have received from people. For people who are new to Facebook, we may have minimal data that we can use. For people who have used our services for longer, we likely have more data, but the amount of data will depend on the nature of that use and how they have used our controls. Any person can see each of the specific interests we maintain about them for advertising by visiting Ads Preferences, which lets people see what interests we use to choose ads for them—and to edit or delete these interests. We also provide more detailed information about how we use data to decide what ads to show to people in our "About Facebook Ads" page, at https://www.facebook.com/ads/about. And, we do not sell people's information to anyone, and we never will.

All users must expressly consent to Facebook's Terms and Data Policy when registering for Facebook. The Data Policy explains the kinds of information we collect, how we use this information, how we share this information, and how users can manage and delete information.

Facebook does not create profiles for people without a Facebook account, but we do receive some information from devices and browsers that may be used by non-users. For example:

- When people visit apps or websites that feature our technologies—like the Facebook Like or Comment button—our servers automatically log (i) standard browser or app records of the fact that a particular device or user visited the website or app (this connection to Facebook's servers occurs automatically when a person visits a website or app that contains our technologies, such as a Like button, and is an inherent function of Internet design); and (ii) any additional information the publisher of the app or website chooses to share with Facebook about the person's activities on that site (such as the fact that a purchase was made on the site). This is a standard feature of the Internet, and most websites and apps share this same information with multiple different third-parties whenever people visit their website or app. When the person visiting a website featuring Facebook's tools is not a registered Facebook user, Facebook does not have information identifying that individual, and it does not create profiles for this individual.

- We also may receive information about the device of a non-registered user if that user visits a part of Facebook that does not require people to log in—such as a public Facebook Page. The information we log when people visit our websites or apps is the

same as described above and is the same information that any provider of an online service would receive.

- In addition, Facebook may receive some basic information about devices where Facebook apps are installed, including before people using those devices have registered for Facebook (such as when a user downloads a Facebook app, but has not yet created an account, or if the app is preloaded on a given device). This device data includes things like device model, operating system, IP address, app version and device identifiers. We use this information to provide the right version of the app, help people who want to create accounts (for example, optimizing the registration flow for the specific device), retrieving bug fixes and measuring and improving app performance. We do not use this information to build profiles about non-registered users.

475. Was his own, his family's, other Execs at FB, etc. personal data also provided/accessed?

Facebook's policies regarding third-party usage of its platform technologies have prohibited—and continue to prohibit—third-party app developers from selling or licensing user data accessed from Facebook and from sharing any user data accessed from Facebook with any ad network, data broker or other advertising or monetization-related service. We take action on potential violations of our Platform Policies based on proactive review, external reports, and other signals. Kogan was not permitted to sell or transfer data to third-parties for the purposes he did. In doing so, Kogan and his company violated Facebook's Platform Policies.

On December 11, 2015, *The Guardian* published an article reporting that Kogan and his company, GSR, may have passed information the app had obtained from Facebook users to SCL Elections Ltd. (SCL)/Cambridge Analytica. Facebook immediately banned Kogan's app from our platform and investigated what happened and what further action Facebook should take to enforce our Platform Policies. Facebook considered the matter closed after obtaining written certifications and confirmations from Kogan, GSR, Cambridge Analytica, and SCL declaring that all such data they had obtained was accounted for and destroyed. We did not have any reason to affirmatively question the veracity of any of these certifications until March 2018, when we learned from media reporting that questions had been raised concerning the accuracy of the certifications. Facebook immediately banned Cambridge Analytica and SCL from purchasing advertisements on our services as well as removed the personal accounts of some of their officers. Moreover, while Facebook's policies in place at the time allowed us to audit apps to ensure that they were safe and did not violate its terms, we had already terminated Kogan's app's access to Facebook. Accordingly, there were no ongoing concerns about the level of data that app could access or might access in the future. With the benefit of hindsight, we wish we had notified people whose information may have been impacted. Facebook has since notified all people potentially impacted with a detailed notice at the top of their News Feed.

476. When will you start paying for the personal data you are stealing??

We believe that it's important to communicate with people about the information that we collect and how people can control it. As explained in our Data Policy, we collect three basic categories of data about people:

(1) data about things people do and share (and who they connect with) on our services;

(2) data about the devices people use to access our services; and

(3) data we receive from partners, including the websites and apps that use our business tools.

We collect information about the people, Pages, accounts, hashtags, and groups users are connected to and how they interact with them across our Products, such as people a user communicates with the most or groups users are part of. We also collect contact information if they choose to upload, sync, or import it from a device (such as an address book or call log or SMS log history), which we use for things like helping them and others find people they may know.

The data we use to show ads to people depends on the data we have received from people. For people who are new to Facebook, we may have minimal data that we can use. For people who have used our services for longer, we likely have more data, but the amount of data will depend on the nature of that use and how they have used our controls. Any person can see each of the specific interests we maintain about them for advertising by visiting Ads Preferences, which lets people see what interests we use to choose ads for them—and to edit or delete these interests. We also provide more detailed information about how we use data to decide what ads to show to people in our "About Facebook Ads" page, at https://www.facebook.com/ads/about. And, we do not sell people's information to anyone, and we never will.

All users must expressly consent to Facebook's Terms and Data Policy when registering for Facebook. The Data Policy explains the kinds of information we collect, how we use this information, how we share this information, and how users can manage and delete information.

Facebook does not create profiles for people without a Facebook account, but we do receive some information from devices and browsers that may be used by non-users. For example:

- When people visit apps or websites that feature our technologies—like the Facebook Like or Comment button—our servers automatically log (i) standard browser or app records of the fact that a particular device or user visited the website or app (this connection to Facebook's servers occurs automatically when a person visits a website or app that contains our technologies, such as a Like button, and is an inherent function of Internet design); and (ii) any additional information the publisher of the app or website chooses to share with Facebook about the person's activities on that site (such as the fact that a purchase was made on the site). This is a standard feature of the Internet, and most websites and apps share this same information with multiple different third-parties whenever people visit their website or app. When the person visiting a website featuring Facebook's tools is not a registered Facebook user, Facebook does not have information identifying that individual, and it does not create profiles for this individual.

- We also may receive information about the device of a non-registered user if that user visits a part of Facebook that does not require people to log in—such as a public

Facebook Page. The information we log when people visit our websites or apps is the same as described above and is the same information that any provider of an online service would receive.

- In addition, Facebook may receive some basic information about devices where Facebook apps are installed, including before people using those devices have registered for Facebook (such as when a user downloads a Facebook app, but has not yet created an account, or if the app is preloaded on a given device). This device data includes things like device model, operating system, IP address, app version and device identifiers. We use this information to provide the right version of the app, help people who want to create accounts (for example, optimizing the registration flow for the specific device), retrieving bug fixes and measuring and improving app performance. We do not use this information to build profiles about non-registered users.

477. How can we retain the benefits of a free press when technology now allows anyone to have a press with tremendous dissemination of information / disinformation?

As discussed with your staff, this question is not germane to the hearing.

478. How is Facebook's problem of information "scraping" different from information gleaned from a person's credit card, banking, and other activity that occurs electronically????

We believe that it's important to communicate with people about the information that we collect and how people can control it. As explained in our Data Policy, we collect three basic categories of data about people:

(1) data about things people do and share (and who they connect with) on our services;

(2) data about the devices people use to access our services; and

(3) data we receive from partners, including the websites and apps that use our business tools.

We collect information about the people, Pages, accounts, hashtags, and groups users are connected to and how they interact with them across our Products, such as people a user communicates with the most or groups users are part of. We also collect contact information if they choose to upload, sync, or import it from a device (such as an address book or call log or SMS log history), which we use for things like helping them and others find people they may know.

The data we use to show ads to people depends on the data we have received from people. For people who are new to Facebook, we may have minimal data that we can use. For people who have used our services for longer, we likely have more data, but the amount of data will depend on the nature of that use and how they have used our controls. Any person can see each of the specific interests we maintain about them for advertising by visiting Ads Preferences, which lets people see what interests we use to choose ads for them—and to edit or delete these interests. We also provide more detailed information about how we use data to decide what ads

to show to people in our "About Facebook Ads" page, at https://www.facebook.com/ads/about. And, we do not sell people's information to anyone, and we never will.

All users must expressly consent to Facebook's Terms and Data Policy when registering for Facebook. The Data Policy explains the kinds of information we collect, how we use this information, how we share this information, and how users can manage and delete information.

Facebook does not create profiles for people without a Facebook account, but we do receive some information from devices and browsers that may be used by non-users. For example:

- When people visit apps or websites that feature our technologies—like the Facebook Like or Comment button—our servers automatically log (i) standard browser or app records of the fact that a particular device or user visited the website or app (this connection to Facebook's servers occurs automatically when a person visits a website or app that contains our technologies, such as a Like button, and is an inherent function of Internet design); and (ii) any additional information the publisher of the app or website chooses to share with Facebook about the person's activities on that site (such as the fact that a purchase was made on the site). This is a standard feature of the Internet, and most websites and apps share this same information with multiple different third-parties whenever people visit their website or app. When the person visiting a website featuring Facebook's tools is not a registered Facebook user, Facebook does not have information identifying that individual, and it does not create profiles for this individual.

- We also may receive information about the device of a non-registered user if that user visits a part of Facebook that does not require people to log in—such as a public Facebook Page. The information we log when people visit our websites or apps is the same as described above and is the same information that any provider of an online service would receive.

- In addition, Facebook may receive some basic information about devices where Facebook apps are installed, including before people using those devices have registered for Facebook (such as when a user downloads a Facebook app, but has not yet created an account, or if the app is preloaded on a given device). This device data includes things like device model, operating system, IP address, app version and device identifiers. We use this information to provide the right version of the app, help people who want to create accounts (for example, optimizing the registration flow for the specific device), retrieving bug fixes and measuring and improving app performance. We do not use this information to build profiles about non-registered users.

479. Zuckerberg should be penalized for lack of sight of his company and have a heavy fine to teach

As discussed with your staff, this question is not germane to the hearing.

480. We are heading down the wrong road. Stop Trump, stop wasting time with honest people.

As discussed with your staff, this question is not germane to the hearing.

481. In your opinion, what constitutes harm?

As discussed with your staff, this question is not germane to the hearing.

482. Only a comment. Thank goodness I deleted my account several years ago.

As discussed with your staff, this question is not germane to the hearing.

483. Who are your paying customers and what are they paying for?

We believe that it's important to communicate with people about the information that we collect and how people can control it. As explained in our Data Policy, we collect three basic categories of data about people:

(1) data about things people do and share (and who they connect with) on our services;

(2) data about the devices people use to access our services; and

(3) data we receive from partners, including the websites and apps that use our business tools.

We collect information about the people, Pages, accounts, hashtags, and groups users are connected to and how they interact with them across our Products, such as people a user communicates with the most or groups users are part of. We also collect contact information if they choose to upload, sync, or import it from a device (such as an address book or call log or SMS log history), which we use for things like helping them and others find people they may know.

The data we use to show ads to people depends on the data we have received from people. For people who are new to Facebook, we may have minimal data that we can use. For people who have used our services for longer, we likely have more data, but the amount of data will depend on the nature of that use and how they have used our controls. Any person can see each of the specific interests we maintain about them for advertising by visiting Ads Preferences, which lets people see what interests we use to choose ads for them—and to edit or delete these interests. We also provide more detailed information about how we use data to decide what ads to show to people in our "About Facebook Ads" page, at https://www.facebook.com/ads/about. And, we do not sell people's information to anyone, and we never will.

All users must expressly consent to Facebook's Terms and Data Policy when registering for Facebook. The Data Policy explains the kinds of information we collect, how we use this information, how we share this information, and how users can manage and delete information.

Facebook does not create profiles for people without a Facebook account, but we do receive some information from devices and browsers that may be used by non-users. For example:

- When people visit apps or websites that feature our technologies—like the Facebook Like or Comment button—our servers automatically log (i) standard browser or app records of the fact that a particular device or user visited the website or app (this connection to Facebook's servers occurs automatically when a person visits a website or app that contains our technologies, such as a Like button, and is an inherent function of Internet design); and (ii) any additional information the publisher of the app or website chooses to share with Facebook about the person's activities on that site (such as the fact that a purchase was made on the site). This is a standard feature of the Internet, and most websites and apps share this same information with multiple different third-parties whenever people visit their website or app. When the person visiting a website featuring Facebook's tools is not a registered Facebook user, Facebook does not have information identifying that individual, and it does not create profiles for this individual.

- We also may receive information about the device of a non-registered user if that user visits a part of Facebook that does not require people to log in—such as a public Facebook Page. The information we log when people visit our websites or apps is the same as described above and is the same information that any provider of an online service would receive.

- In addition, Facebook may receive some basic information about devices where Facebook apps are installed, including before people using those devices have registered for Facebook (such as when a user downloads a Facebook app, but has not yet created an account, or if the app is preloaded on a given device). This device data includes things like device model, operating system, IP address, app version and device identifiers. We use this information to provide the right version of the app, help people who want to create accounts (for example, optimizing the registration flow for the specific device), retrieving bug fixes and measuring and improving app performance. We do not use this information to build profiles about non-registered users.

484. Do you think you will be able to solve the problems? If so, how?

We believe everyone deserves good privacy controls. A user owns the information they share on Facebook. This means they decide what they share and who they share it with on Facebook, and they can change their mind. We require websites and apps who use our tools to tell users they're collecting and sharing their information with us, and to get users' permission to do so.

Everyone has the right to expect strong protections for their information. We also need to do our part to help keep our community safe, in a way that's consistent with people's privacy expectations. We've recently announced several steps to give people more control over their privacy, including a new Privacy Shortcuts tool that we're rolling out now to give people information about how to control their information, including choosing who can see what they post and adding protections like two-factor authentication to their account. People can learn more about how to protect their privacy in our updated Data Policy and in our Privacy Basics feature (https://www.facebook.com/about/basics).

We are in the process of investigating every app that had access to a large amount of information before we changed our Platform in 2014. The investigation process is in full swing. We have large teams of internal and external experts working hard to investigate these apps as quickly as possible. As of early June 2018, thousands of apps have been investigated and around 200 apps have been suspended—pending a thorough investigation into whether they did in fact misuse any data. Where we find evidence that these or other apps did misuse data, we will ban them and let people know.

Facebook is generally not opposed to regulation but wants to ensure it is the right regulation. The issues facing the industry are complex, multi-faceted, and affect an important part of peoples' lives. As such, Facebook is absolutely committed to working with regulators, like Congress, to craft the right regulations. Facebook would be happy to review any proposed legislation and provide comments.

485. Have you ever turned down advertisers or third parties data was being sold to due to ethics concerns?

To build a secure product with extensive infrastructure that connects people wherever they live or whatever their income level, we need to make sure everyone can afford it. Advertising lets us keep Facebook free, which ensures it remains affordable for everyone. We also believe the ads you see across the Facebook family of apps and services should be useful and relevant to you. Users can't opt out of seeing ads altogether because selling ads is what keeps Facebook free, but they do have different options to control how their data can and can't be used to show them ads. They're all found in ad preferences, which allows users to turn off the use of all data collected from partners off Facebook to target ads. Users can also decide which of their profile fields they want used for ad targeting in the Information section under "About you." Users can remove themselves from interests under "Your interests" and categories under "Your categories." And, we do not sell people's information to anyone, and we never will.

Facebook is committed to transparency for all ads, including ads with political content. Facebook believes that people should be able to easily understand why they are seeing ads, who paid for them, and what other ads those advertisers are running. As such, Facebook only allows authorized advertisers to run ads about elections or issues that are being debated across the country. In order to be authorized by Facebook, advertisers will need to confirm their identity and location. Furthermore, all political and issue ads will include a disclosure which reads: "Paid for by," and when users click on this disclosure they will be able to see details about the advertiser. Users will also be able to see an explanation of why they saw the particular ad. This is similar to the disclosure included on political TV advertisements. We just launched globally View Active Ads, a feature that will enable anyone to see all of the ads an advertiser is currently running by visiting the advertiser's Facebook Page.

486. Why did you wait till Facebook stock was effected to take action on the data breach?

Facebook's policies regarding third-party usage of its platform technologies have prohibited—and continue to prohibit—third-party app developers from selling or licensing user data accessed from Facebook and from sharing any user data accessed from Facebook with any

ad network, data broker or other advertising or monetization-related service. We take action on potential violations of our Platform Policies based on proactive review, external reports, and other signals. Kogan was not permitted to sell or transfer data to third-parties for the purposes he did. In doing so, Kogan and his company violated Facebook's Platform Policies.

On December 11, 2015, *The Guardian* published an article reporting that Kogan and his company, GSR, may have passed information the app had obtained from Facebook users to SCL Elections Ltd. (SCL)/Cambridge Analytica. Facebook immediately banned Kogan's app from our platform and investigated what happened and what further action Facebook should take to enforce our Platform Policies. Facebook considered the matter closed after obtaining written certifications and confirmations from Kogan, GSR, Cambridge Analytica, and SCL declaring that all such data they had obtained was accounted for and destroyed. We did not have any reason to affirmatively question the veracity of any of these certifications until March 2018, when we learned from media reporting that questions had been raised concerning the accuracy of the certifications. Facebook immediately banned Cambridge Analytica and SCL from purchasing advertisements on our services as well as removed the personal accounts of some of their officers. Moreover, while Facebook's policies in place at the time allowed us to audit apps to ensure that they were safe and did not violate its terms, we had already terminated Kogan's app's access to Facebook. Accordingly, there were no ongoing concerns about the level of data that app could access or might access in the future. With the benefit of hindsight, we wish we had notified people whose information may have been impacted. Facebook has since notified all people potentially impacted with a detailed notice at the top of their News Feed.

487. How much is people's private info worth to you?

We believe that it's important to communicate with people about the information that we collect and how people can control it. As explained in our Data Policy, we collect three basic categories of data about people:

(1) data about things people do and share (and who they connect with) on our services;

(2) data about the devices people use to access our services; and

(3) data we receive from partners, including the websites and apps that use our business tools.

We collect information about the people, Pages, accounts, hashtags, and groups users are connected to and how they interact with them across our Products, such as people a user communicates with the most or groups users are part of. We also collect contact information if they choose to upload, sync, or import it from a device (such as an address book or call log or SMS log history), which we use for things like helping them and others find people they may know.

The data we use to show ads to people depends on the data we have received from people. For people who are new to Facebook, we may have minimal data that we can use. For people who have used our services for longer, we likely have more data, but the amount of data will depend on the nature of that use and how they have used our controls. Any person can see each of the specific interests we maintain about them for advertising by visiting Ads Preferences,

which lets people see what interests we use to choose ads for them—and to edit or delete these interests. We also provide more detailed information about how we use data to decide what ads to show to people in our "About Facebook Ads" page, at https://www.facebook.com/ads/about. And, we do not sell people's information to anyone, and we never will.

All users must expressly consent to Facebook's Terms and Data Policy when registering for Facebook. The Data Policy explains the kinds of information we collect, how we use this information, how we share this information, and how users can manage and delete information.

Facebook does not create profiles for people without a Facebook account, but we do receive some information from devices and browsers that may be used by non-users. For example:

- When people visit apps or websites that feature our technologies—like the Facebook Like or Comment button—our servers automatically log (i) standard browser or app records of the fact that a particular device or user visited the website or app (this connection to Facebook's servers occurs automatically when a person visits a website or app that contains our technologies, such as a Like button, and is an inherent function of Internet design); and (ii) any additional information the publisher of the app or website chooses to share with Facebook about the person's activities on that site (such as the fact that a purchase was made on the site). This is a standard feature of the Internet, and most websites and apps share this same information with multiple different third-parties whenever people visit their website or app. When the person visiting a website featuring Facebook's tools is not a registered Facebook user, Facebook does not have information identifying that individual, and it does not create profiles for this individual.

- We also may receive information about the device of a non-registered user if that user visits a part of Facebook that does not require people to log in—such as a public Facebook Page. The information we log when people visit our websites or apps is the same as described above and is the same information that any provider of an online service would receive.

- In addition, Facebook may receive some basic information about devices where Facebook apps are installed, including before people using those devices have registered for Facebook (such as when a user downloads a Facebook app, but has not yet created an account, or if the app is preloaded on a given device). This device data includes things like device model, operating system, IP address, app version and device identifiers. We use this information to provide the right version of the app, help people who want to create accounts (for example, optimizing the registration flow for the specific device), retrieving bug fixes and measuring and improving app performance. We do not use this information to build profiles about non-registered users.

488. Why did Facebook collect and share text messages and phone call data from user phones?

We believe that it's important to communicate with people about the information that we collect and how people can control it. As explained in our Data Policy, we collect three basic categories of data about people:

(1) data about things people do and share (and who they connect with) on our services;

(2) data about the devices people use to access our services; and

(3) data we receive from partners, including the websites and apps that use our business tools.

We collect information about the people, Pages, accounts, hashtags, and groups users are connected to and how they interact with them across our Products, such as people a user communicates with the most or groups users are part of. We also collect contact information if they choose to upload, sync, or import it from a device (such as an address book or call log or SMS log history), which we use for things like helping them and others find people they may know.

The data we use to show ads to people depends on the data we have received from people. For people who are new to Facebook, we may have minimal data that we can use. For people who have used our services for longer, we likely have more data, but the amount of data will depend on the nature of that use and how they have used our controls. Any person can see each of the specific interests we maintain about them for advertising by visiting Ads Preferences, which lets people see what interests we use to choose ads for them—and to edit or delete these interests. We also provide more detailed information about how we use data to decide what ads to show to people in our "About Facebook Ads" page, at https://www.facebook.com/ads/about. And, we do not sell people's information to anyone, and we never will.

All users must expressly consent to Facebook's Terms and Data Policy when registering for Facebook. The Data Policy explains the kinds of information we collect, how we use this information, how we share this information, and how users can manage and delete information.

Facebook does not create profiles for people without a Facebook account, but we do receive some information from devices and browsers that may be used by non-users. For example:

- When people visit apps or websites that feature our technologies—like the Facebook Like or Comment button—our servers automatically log (i) standard browser or app records of the fact that a particular device or user visited the website or app (this connection to Facebook's servers occurs automatically when a person visits a website or app that contains our technologies, such as a Like button, and is an inherent function of Internet design); and (ii) any additional information the publisher of the app or website chooses to share with Facebook about the person's activities on that site (such as the fact that a purchase was made on the site). This is a standard feature of the Internet, and most websites and apps share this same information with multiple different third-parties whenever people visit their website or app. When the person visiting a website featuring

Facebook's tools is not a registered Facebook user, Facebook does not have information identifying that individual, and it does not create profiles for this individual.

- We also may receive information about the device of a non-registered user if that user visits a part of Facebook that does not require people to log in—such as a public Facebook Page. The information we log when people visit our websites or apps is the same as described above and is the same information that any provider of an online service would receive.

- In addition, Facebook may receive some basic information about devices where Facebook apps are installed, including before people using those devices have registered for Facebook (such as when a user downloads a Facebook app, but has not yet created an account, or if the app is preloaded on a given device). This device data includes things like device model, operating system, IP address, app version and device identifiers. We use this information to provide the right version of the app, help people who want to create accounts (for example, optimizing the registration flow for the specific device), retrieving bug fixes and measuring and improving app performance. We do not use this information to build profiles about non-registered users.

489. The most pressing question of our time is what is the truth and what is a fact, how will you ensure your platform is a vessel for truth?

We want Facebook to be a place where people can discover more news, information, and perspectives, and we are working to build products that help to that. Through our News Feed algorithm, we also work hard to actively reduce the distribution of clickbait, sensationalism, and misinformation, on the one hand, and to boost news and information from sources that are trusted, informative, and local, on the other hand.

We are focusing on four different strategies to address misinformation:

- **Strengthening enforcement of our authenticity policies.** We are investing heavily in new technology and hiring thousands more people to tackle the problem of inauthenticity on the platform. Fake accounts are often associated with false news, so this is an area that will have a huge impact on curbing the spread of inaccurate information.

- **Finding industry solutions.** All of us—from tech companies and media companies to newsrooms and classrooms—must work together to find industry solutions to strengthen the online news ecosystem and our own digital literacy. That's why we're collaborating with others who operate in this space. Last January, we announced The Facebook Journalism Project, an initiative that seeks to establish stronger ties between Facebook and the news industry. The project is focused on developing news products, providing training and tools for journalists, and working with publishers and educators on how we can equip people with the knowledge they need to be informed readers in the digital age. Since launching the Journalism Project, we've met with more than 2,600 publishers around the world to understand how they use our products and how we can make improvements to better support their needs.

- **Disrupting economic incentives.** When it comes to fighting false news, we've found that a lot of it is financially motivated. So, one of the most effective approaches is removing the economic incentives for those who traffic in inaccurate information. We've done things like block ads from pages that repeatedly share false news and significantly limit the distribution of web pages that deliver low quality web experiences.

- **Building new products.** We believe it's important to amplify the good effects of social media and mitigate the bad—to contribute to the diversity of ideas, information, and view points, while strengthening our common understanding.

    - We believe giving people more context can help them decide what to trust and what to share. The third-party fact-checking program we have developed uses reports from our community, along with other signals, to send stories to accredited third-party fact checking organizations. If the fact checking organizations identify a story as fake, we will suggest related articles in News Feed to show people different points of view, including information from fact checkers. Stories that have been disputed may also appear lower in News Feed. Our own data analytics show that a false rating from one of our fact checking partners reduces future impressions on Facebook by 80 percent.

    - We're also testing Article Context as a way of giving people more information about the material they're reading on Facebook. Since we launched this test, some of the articles people see in News Feed will feature an "i" icon that allows them to access more information at the tap of a button. The information we surface is pulled from across the internet, and includes things like the publisher's Wikipedia entry, trending articles or related articles about the topic, and information about how the article is being shared on Facebook. In some cases, if that information is unavailable, we will let people know since that can also be helpful context.

490. Why did he not fix this problem when he knew about it years ago?

Facebook's policies regarding third-party usage of its platform technologies have prohibited—and continue to prohibit—third-party app developers from selling or licensing user data accessed from Facebook and from sharing any user data accessed from Facebook with any ad network, data broker or other advertising or monetization-related service. We take action on potential violations of our Platform Policies based on proactive review, external reports, and other signals. Kogan was not permitted to sell or transfer data to third-parties for the purposes he did. In doing so, Kogan and his company violated Facebook's Platform Policies.

On December 11, 2015, *The Guardian* published an article reporting that Kogan and his company, GSR, may have passed information the app had obtained from Facebook users to SCL Elections Ltd. (SCL)/Cambridge Analytica. Facebook immediately banned Kogan's app from our platform and investigated what happened and what further action Facebook should take to enforce our Platform Policies. Facebook considered the matter closed after obtaining written certifications and confirmations from Kogan, GSR, Cambridge Analytica, and SCL declaring

that all such data they had obtained was accounted for and destroyed. We did not have any reason to affirmatively question the veracity of any of these certifications until March 2018, when we learned from media reporting that questions had been raised concerning the accuracy of the certifications. Facebook immediately banned Cambridge Analytica and SCL from purchasing advertisements on our services as well as removed the personal accounts of some of their officers. Moreover, while Facebook's policies in place at the time allowed us to audit apps to ensure that they were safe and did not violate its terms, we had already terminated Kogan's app's access to Facebook. Accordingly, there were no ongoing concerns about the level of data that app could access or might access in the future. With the benefit of hindsight, we wish we had notified people whose information may have been impacted. Facebook has since notified all people potentially impacted with a detailed notice at the top of their News Feed.

491. Why aren't you getting out of selling personal info? & doing subscriptions instead?

We believe that it's important to communicate with people about the information that we collect and how people can control it. As explained in our Data Policy, we collect three basic categories of data about people:

(1) data about things people do and share (and who they connect with) on our services;

(2) data about the devices people use to access our services; and

(3) data we receive from partners, including the websites and apps that use our business tools.

We collect information about the people, Pages, accounts, hashtags, and groups users are connected to and how they interact with them across our Products, such as people a user communicates with the most or groups users are part of. We also collect contact information if they choose to upload, sync, or import it from a device (such as an address book or call log or SMS log history), which we use for things like helping them and others find people they may know.

The data we use to show ads to people depends on the data we have received from people. For people who are new to Facebook, we may have minimal data that we can use. For people who have used our services for longer, we likely have more data, but the amount of data will depend on the nature of that use and how they have used our controls. Any person can see each of the specific interests we maintain about them for advertising by visiting Ads Preferences, which lets people see what interests we use to choose ads for them—and to edit or delete these interests. We also provide more detailed information about how we use data to decide what ads to show to people in our "About Facebook Ads" page, at https://www.facebook.com/ads/about. And, we do not sell people's information to anyone, and we never will.

All users must expressly consent to Facebook's Terms and Data Policy when registering for Facebook. The Data Policy explains the kinds of information we collect, how we use this information, how we share this information, and how users can manage and delete information.

Facebook does not create profiles for people without a Facebook account, but we do receive some information from devices and browsers that may be used by non-users. For example:

- When people visit apps or websites that feature our technologies—like the Facebook Like or Comment button—our servers automatically log (i) standard browser or app records of the fact that a particular device or user visited the website or app (this connection to Facebook's servers occurs automatically when a person visits a website or app that contains our technologies, such as a Like button, and is an inherent function of Internet design); and (ii) any additional information the publisher of the app or website chooses to share with Facebook about the person's activities on that site (such as the fact that a purchase was made on the site). This is a standard feature of the Internet, and most websites and apps share this same information with multiple different third-parties whenever people visit their website or app. When the person visiting a website featuring Facebook's tools is not a registered Facebook user, Facebook does not have information identifying that individual, and it does not create profiles for this individual.

- We also may receive information about the device of a non-registered user if that user visits a part of Facebook that does not require people to log in—such as a public Facebook Page. The information we log when people visit our websites or apps is the same as described above and is the same information that any provider of an online service would receive.

- In addition, Facebook may receive some basic information about devices where Facebook apps are installed, including before people using those devices have registered for Facebook (such as when a user downloads a Facebook app, but has not yet created an account, or if the app is preloaded on a given device). This device data includes things like device model, operating system, IP address, app version and device identifiers. We use this information to provide the right version of the app, help people who want to create accounts (for example, optimizing the registration flow for the specific device), retrieving bug fixes and measuring and improving app performance. We do not use this information to build profiles about non-registered users.

492. Will he support my safety by defunding sanctuary cities and cooperate with ICE

As discussed with your staff, this question is not germane to the hearing.

493. Your site helped elect Pres Trump! Are you going to help get him impeached?

As discussed with your staff, this question is not germane to the hearing.

494. In our "Buyer/User Beware" world we live in how does and why should you company protect the personal

We believe everyone deserves good privacy controls. A user owns the information they share on Facebook. This means they decide what they share and who they share it with on Facebook, and they can change their mind. We require websites and apps who use our tools to

tell users they're collecting and sharing their information with us, and to get users' permission to do so.

Everyone has the right to expect strong protections for their information. We also need to do our part to help keep our community safe, in a way that's consistent with people's privacy expectations. We've recently announced several steps to give people more control over their privacy, including a new Privacy Shortcuts tool that we're rolling out now to give people information about how to control their information, including choosing who can see what they post and adding protections like two-factor authentication to their account. People can learn more about how to protect their privacy in our updated Data Policy and in our Privacy Basics feature (https://www.facebook.com/about/basics).

We are in the process of investigating every app that had access to a large amount of information before we changed our Platform in 2014. The investigation process is in full swing. We have large teams of internal and external experts working hard to investigate these apps as quickly as possible. As of early June 2018, thousands of apps have been investigated and around 200 apps have been suspended—pending a thorough investigation into whether they did in fact misuse any data. Where we find evidence that these or other apps did misuse data, we will ban them and let people know.

Facebook is generally not opposed to regulation but wants to ensure it is the right regulation. The issues facing the industry are complex, multi-faceted, and affect an important part of peoples' lives. As such, Facebook is absolutely committed to working with regulators, like Congress, to craft the right regulations. Facebook would be happy to review any proposed legislation and provide comments.

495. What are dos & don'ts you recommend people use on social media? Can they pay for their privacy?

We believe everyone deserves good privacy controls. A user owns the information they share on Facebook. This means they decide what they share and who they share it with on Facebook, and they can change their mind. We require websites and apps who use our tools to tell users they're collecting and sharing their information with us, and to get users' permission to do so.

Everyone has the right to expect strong protections for their information. We also need to do our part to help keep our community safe, in a way that's consistent with people's privacy expectations. We've recently announced several steps to give people more control over their privacy, including a new Privacy Shortcuts tool that we're rolling out now to give people information about how to control their information, including choosing who can see what they post and adding protections like two-factor authentication to their account. People can learn more about how to protect their privacy in our updated Data Policy and in our Privacy Basics feature (https://www.facebook.com/about/basics).

We are in the process of investigating every app that had access to a large amount of information before we changed our Platform in 2014. The investigation process is in full swing. We have large teams of internal and external experts working hard to investigate these apps as

quickly as possible. As of early June 2018, thousands of apps have been investigated and around 200 apps have been suspended—pending a thorough investigation into whether they did in fact misuse any data. Where we find evidence that these or other apps did misuse data, we will ban them and let people know.

Facebook is generally not opposed to regulation but wants to ensure it is the right regulation. The issues facing the industry are complex, multi-faceted, and affect an important part of peoples' lives. As such, Facebook is absolutely committed to working with regulators, like Congress, to craft the right regulations. Facebook would be happy to review any proposed legislation and provide comments.

496. Why did you not fire or suspend your VP who wrote/comments about life or death at the time, what were your comments to him back then when he did this? For only now u are opposed when u have been exposed?

We recognize that we have made mistakes, and we are committed to learning from this experience to secure our platform further and make our community safer for everyone going forward. As our CEO Mark Zuckerberg has said, when you are building something unprecedented like Facebook, there are going to be mistakes. What people should hold us accountable for is learning from the mistakes and continually doing better—and, at the end of the day, making sure that we're building things that people like and that make their lives better.

Particularly in the past few months, we've realized that we need to take a broader view of our responsibility to our community. Part of that effort is continuing our ongoing efforts to identify ways that we can improve our privacy practices. We've heard loud and clear that privacy settings and other important tools are too hard to find and that we must do more to keep people informed. So, we're taking additional steps to put people more in control of their privacy. For instance, we redesigned our entire settings menu on mobile devices from top to bottom to make things easier to find. We also created a new Privacy Shortcuts in a menu where users can control their data in just a few taps, with clearer explanations of how our controls work. The experience is now clearer, more visual, and easy-to-find. Furthermore, we also updated our terms of service that include our commitments to everyone using Facebook. We explain the services we offer in language that's easier to read. We've also updated our Data Policy to better spell out what data we collect and how we use it in Facebook, Instagram, Messenger, and other products.

497. Is there any privacy on the internet at all? Please explain.

We believe everyone deserves good privacy controls. A user owns the information they share on Facebook. This means they decide what they share and who they share it with on Facebook, and they can change their mind. We require websites and apps who use our tools to tell users they're collecting and sharing their information with us, and to get users' permission to do so.

Everyone has the right to expect strong protections for their information. We also need to do our part to help keep our community safe, in a way that's consistent with people's privacy expectations. We've recently announced several steps to give people more control over their privacy, including a new Privacy Shortcuts tool that we're rolling out now to give people

information about how to control their information, including choosing who can see what they post and adding protections like two-factor authentication to their account. People can learn more about how to protect their privacy in our updated Data Policy and in our Privacy Basics feature (https://www.facebook.com/about/basics).

We are in the process of investigating every app that had access to a large amount of information before we changed our Platform in 2014. The investigation process is in full swing. We have large teams of internal and external experts working hard to investigate these apps as quickly as possible. As of early June 2018, thousands of apps have been investigated and around 200 apps have been suspended—pending a thorough investigation into whether they did in fact misuse any data. Where we find evidence that these or other apps did misuse data, we will ban them and let people know.

Facebook is generally not opposed to regulation but wants to ensure it is the right regulation. The issues facing the industry are complex, multi-faceted, and affect an important part of peoples' lives. As such, Facebook is absolutely committed to working with regulators, like Congress, to craft the right regulations. Facebook would be happy to review any proposed legislation and provide comments.

498. Has FB grown too big to control? Should it be considered a utility and broken into smaller companies?

Protecting people's data is one of our most important responsibilities, and we are committed to continuing our work to improve how we protect people's information and to working with regulators to draft appropriate regulations. Our mission is to give people the power to build community and bring the world closer together. As the internet becomes more important in people's lives, the real question is about the right set of regulations that should apply to all internet services, regardless of size. Across the board, we have a responsibility to not just build tools, but to make sure that they're used in ways that are positive for our users. Facebook is generally not opposed to regulation but wants to ensure it is the right regulation. The issues facing the industry are complex, multi-faceted, and affect an important part of peoples' lives. As such, Facebook is absolutely committed to working with regulators, like Congress, to craft the right regulations.

We are already regulated in many ways—for example, under the Federal Trade Commission Act—and we are subject to ongoing oversight by the FTC under the terms of a 2011 consent order. We furnished extensive information to the FTC regarding the ability for users to port their Facebook data (including friends data that had been shared with them) with apps on Facebook's platform, as part of the FTC's investigation culminating in the July 27, 2012 Consent Order. The Consent Order memorializes the agreement between Facebook and the FTC and did not require Facebook to turn off or change the ability for people to port friends data that had been shared with them on Facebook to apps they used. Facebook voluntarily changed this feature of Platform in 2014, however. Facebook has not violated the Federal Trade Commission Act. Facebook is not in a position to determine whether third-party app developers violated the Act and leaves that determination to the FTC, although we can confirm that misrepresenting the terms of an app to users is a violation of Facebook's developer policies.

Facebook has inherent incentives to protect its customers' privacy and address breaches and vulnerabilities. Indeed, the recent discovery of misconduct by an app developer on the Facebook platform clearly hurt Facebook and made it harder for us to achieve our social mission. As such, Facebook is committed to protecting our platform from bad actors, ensuring we are able to continue our mission of giving people a voice and bringing them closer together. It will take some time to work through all the changes we need to make across the company, but Facebook is committed to getting this right.

499. How can Facebook safeguards be trusted, given irreparable damage already done and cover-up

Facebook's policies regarding third-party usage of its platform technologies have prohibited—and continue to prohibit—third-party app developers from selling or licensing user data obtained from Facebook and from sharing any user data obtained from Facebook with any ad network, data broker or other advertising or monetization-related service.

We use a variety of tools to enforce Facebook policies against violating parties, including developers. We review tens of thousands of apps per year and regularly disapprove noncompliant apps as part of our proactive review process. We also use tools like cease and desist letters, account suspensions, letter agreements, and civil litigation. For example, since 2006, Facebook has sent over 1,150 cease-and-desist letters to over 1,600 targets. In 2017, we took action against about 370,000 apps, ranging from imposing certain restrictions to removal of the app from the platform. Moreover, we have required parties who have procured our data without authorization to delete that data. We have invested significant resources in these efforts.

Recently, we announced a number of additional steps we're taking to address concerns raised by Kogan's app.

- **Review our platform.** We will investigate all apps that had access to large amounts of data before the platform changes we announced in 2014, and we will audit any app where we identify suspicious activity. If we identify misuses of data, we'll take immediate action, including banning the app from our platform and pursuing legal action if appropriate.

- **Tell people about data misuse.** We will tell people about apps that have misused their data. This includes building a way for people to know if their data might have been accessed via the app. Moving forward, if we remove an app, we will tell people.

- **Turn off access for unused apps.** If someone has not used an app within the last three months, we will turn off the app's access to their data.

- **Restrict Facebook Login data.** We are changing Login, so that the only data that an app can request without app review will include name, profile photo, and email address. Requesting any other data will require approval from Facebook. We will also no longer allow apps to ask for access to information like religious or political views, relationship status and details, custom friends lists, education and work history, fitness activity, book reading and music listening activity, news reading, video watch activity, and games

activity. We will encourage people to manage the apps they use. We already show people what apps their accounts are connected to and allow them to control what data they've permitted those apps to use. But we're making it easier for people to see what apps they use and the information they have shared with those apps.

- **Reward people who find vulnerabilities.** We launched the Data Abuse Bounty program so that people can report to us any misuses of data by app developers.

- **Update our policies.** We have updated our terms and Data Policy to explain how we use data and how data is shared with app developers.

500. Please explain why you feel it acceptable to track individuals who have never signed up for Facebook

We believe that it's important to communicate with people about the information that we collect and how people can control it. As explained in our Data Policy, we collect three basic categories of data about people:

(1) data about things people do and share (and who they connect with) on our services;

(2) data about the devices people use to access our services; and

(3) data we receive from partners, including the websites and apps that use our business tools.

We collect information about the people, Pages, accounts, hashtags, and groups users are connected to and how they interact with them across our Products, such as people a user communicates with the most or groups users are part of. We also collect contact information if they choose to upload, sync, or import it from a device (such as an address book or call log or SMS log history), which we use for things like helping them and others find people they may know.

The data we use to show ads to people depends on the data we have received from people. For people who are new to Facebook, we may have minimal data that we can use. For people who have used our services for longer, we likely have more data, but the amount of data will depend on the nature of that use and how they have used our controls. Any person can see each of the specific interests we maintain about them for advertising by visiting Ads Preferences, which lets people see what interests we use to choose ads for them—and to edit or delete these interests. We also provide more detailed information about how we use data to decide what ads to show to people in our "About Facebook Ads" page, at https://www.facebook.com/ads/about. And, we do not sell people's information to anyone, and we never will.

All users must expressly consent to Facebook's Terms and Data Policy when registering for Facebook. The Data Policy explains the kinds of information we collect, how we use this information, how we share this information, and how users can manage and delete information.

Facebook does not create profiles for people without a Facebook account, but we do receive some information from devices and browsers that may be used by non-users. For example:

- When people visit apps or websites that feature our technologies—like the Facebook Like or Comment button—our servers automatically log (i) standard browser or app records of the fact that a particular device or user visited the website or app (this connection to Facebook's servers occurs automatically when a person visits a website or app that contains our technologies, such as a Like button, and is an inherent function of Internet design); and (ii) any additional information the publisher of the app or website chooses to share with Facebook about the person's activities on that site (such as the fact that a purchase was made on the site). This is a standard feature of the Internet, and most websites and apps share this same information with multiple different third-parties whenever people visit their website or app. When the person visiting a website featuring Facebook's tools is not a registered Facebook user, Facebook does not have information identifying that individual, and it does not create profiles for this individual.

- We also may receive information about the device of a non-registered user if that user visits a part of Facebook that does not require people to log in—such as a public Facebook Page. The information we log when people visit our websites or apps is the same as described above and is the same information that any provider of an online service would receive.

- In addition, Facebook may receive some basic information about devices where Facebook apps are installed, including before people using those devices have registered for Facebook (such as when a user downloads a Facebook app, but has not yet created an account, or if the app is preloaded on a given device). This device data includes things like device model, operating system, IP address, app version and device identifiers. We use this information to provide the right version of the app, help people who want to create accounts (for example, optimizing the registration flow for the specific device), retrieving bug fixes and measuring and improving app performance. We do not use this information to build profiles about non-registered users.

501. Today I opened my iPhone, a screen loaded touting NEW Camera, the full screen of my phone looked like an iPhone camera, click here to accept, it wasn't apple it was Facebook. Yet another example of how easy it is to be led into relinquishing control of my personal information with absolutely no context of the magnitude that a simple click accomplishes. Apparently when I previously used the phone I was reviewing friend posts in Facebook, I don't share, I post frugally within my close friend circles yet I am constantly exposed to traps not Facebook alone but given the current situation I would think Facebook would be more thoughtful in launching new features without some sort of disclaimer... no place on the 'camera' update did it say Facebook.

As discussed with your staff, this question is not germane to the hearing.

502. How would you feel, Mark, if you knew your information was in the hands of a malicious third party?

Facebook's policies regarding third-party usage of its platform technologies have prohibited—and continue to prohibit—third-party app developers from selling or licensing user data accessed from Facebook and from sharing any user data accessed from Facebook with any ad network, data broker or other advertising or monetization-related service. We take action on potential violations of our Platform Policies based on proactive review, external reports, and other signals. Kogan was not permitted to sell or transfer data to third-parties for the purposes he did. In doing so, Kogan and his company violated Facebook's Platform Policies.

On December 11, 2015, *The Guardian* published an article reporting that Kogan and his company, GSR, may have passed information the app had obtained from Facebook users to SCL Elections Ltd. (SCL)/Cambridge Analytica. Facebook immediately banned Kogan's app from our platform and investigated what happened and what further action Facebook should take to enforce our Platform Policies. Facebook considered the matter closed after obtaining written certifications and confirmations from Kogan, GSR, Cambridge Analytica, and SCL declaring that all such data they had obtained was accounted for and destroyed. We did not have any reason to affirmatively question the veracity of any of these certifications until March 2018, when we learned from media reporting that questions had been raised concerning the accuracy of the certifications. Facebook immediately banned Cambridge Analytica and SCL from purchasing advertisements on our services as well as removed the personal accounts of some of their officers. Moreover, while Facebook's policies in place at the time allowed us to audit apps to ensure that they were safe and did not violate its terms, we had already terminated Kogan's app's access to Facebook. Accordingly, there were no ongoing concerns about the level of data that app could access or might access in the future. With the benefit of hindsight, we wish we had notified people whose information may have been impacted. Facebook has since notified all people potentially impacted with a detailed notice at the top of their News Feed.

503. No question but recommend that this company be regulated like the media company that it is.

Protecting people's data is one of our most important responsibilities, and we are committed to continuing our work to improve how we protect people's information and to working with regulators to draft appropriate regulations. Our mission is to give people the power to build community and bring the world closer together. As the internet becomes more important in people's lives, the real question is about the right set of regulations that should apply to all internet services, regardless of size. Across the board, we have a responsibility to not just build tools, but to make sure that they're used in ways that are positive for our users. Facebook is generally not opposed to regulation but wants to ensure it is the right regulation. The issues facing the industry are complex, multi-faceted, and affect an important part of peoples' lives. As such, Facebook is absolutely committed to working with regulators, like Congress, to craft the right regulations.

We are already regulated in many ways—for example, under the Federal Trade Commission Act—and we are subject to ongoing oversight by the FTC under the terms of a 2011 consent order. We furnished extensive information to the FTC regarding the ability for users to

port their Facebook data (including friends data that had been shared with them) with apps on Facebook's platform, as part of the FTC's investigation culminating in the July 27, 2012 Consent Order. The Consent Order memorializes the agreement between Facebook and the FTC and did not require Facebook to turn off or change the ability for people to port friends data that had been shared with them on Facebook to apps they used. Facebook voluntarily changed this feature of Platform in 2014, however. Facebook has not violated the Federal Trade Commission Act. Facebook is not in a position to determine whether third-party app developers violated the Act and leaves that determination to the FTC, although we can confirm that misrepresenting the terms of an app to users is a violation of Facebook's developer policies.

Facebook has inherent incentives to protect its customers' privacy and address breaches and vulnerabilities. Indeed, the recent discovery of misconduct by an app developer on the Facebook platform clearly hurt Facebook and made it harder for us to achieve our social mission. As such, Facebook is committed to protecting our platform from bad actors, ensuring we are able to continue our mission of giving people a voice and bringing them closer together. It will take some time to work through all the changes we need to make across the company, but Facebook is committed to getting this right.

504. Why should you not be in prison?

We recognize that we have made mistakes, and we are committed to learning from this experience to secure our platform further and make our community safer for everyone going forward. As our CEO Mark Zuckerberg has said, when you are building something unprecedented like Facebook, there are going to be mistakes. What people should hold us accountable for is learning from the mistakes and continually doing better—and, at the end of the day, making sure that we're building things that people like and that make their lives better.

Particularly in the past few months, we've realized that we need to take a broader view of our responsibility to our community. Part of that effort is continuing our ongoing efforts to identify ways that we can improve our privacy practices. We've heard loud and clear that privacy settings and other important tools are too hard to find and that we must do more to keep people informed. So, we're taking additional steps to put people more in control of their privacy. For instance, we redesigned our entire settings menu on mobile devices from top to bottom to make things easier to find. We also created a new Privacy Shortcuts in a menu where users can control their data in just a few taps, with clearer explanations of how our controls work. The experience is now clearer, more visual, and easy-to-find. Furthermore, we also updated our terms of service that include our commitments to everyone using Facebook. We explain the services we offer in language that's easier to read. We've also updated our Data Policy to better spell out what data we collect and how we use it in Facebook, Instagram, Messenger, and other products.

505. Could Facebook be a social network where we are the customer not the product?

We believe that it's important to communicate with people about the information that we collect and how people can control it. As explained in our Data Policy, we collect three basic categories of data about people:

(1) data about things people do and share (and who they connect with) on our services;

(2) data about the devices people use to access our services; and

(3) data we receive from partners, including the websites and apps that use our business tools.

We collect information about the people, Pages, accounts, hashtags, and groups users are connected to and how they interact with them across our Products, such as people a user communicates with the most or groups users are part of. We also collect contact information if they choose to upload, sync, or import it from a device (such as an address book or call log or SMS log history), which we use for things like helping them and others find people they may know.

The data we use to show ads to people depends on the data we have received from people. For people who are new to Facebook, we may have minimal data that we can use. For people who have used our services for longer, we likely have more data, but the amount of data will depend on the nature of that use and how they have used our controls. Any person can see each of the specific interests we maintain about them for advertising by visiting Ads Preferences, which lets people see what interests we use to choose ads for them—and to edit or delete these interests. We also provide more detailed information about how we use data to decide what ads to show to people in our "About Facebook Ads" page, at https://www.facebook.com/ads/about. And, we do not sell people's information to anyone, and we never will.

All users must expressly consent to Facebook's Terms and Data Policy when registering for Facebook. The Data Policy explains the kinds of information we collect, how we use this information, how we share this information, and how users can manage and delete information.

Facebook does not create profiles for people without a Facebook account, but we do receive some information from devices and browsers that may be used by non-users. For example:

- When people visit apps or websites that feature our technologies—like the Facebook Like or Comment button—our servers automatically log (i) standard browser or app records of the fact that a particular device or user visited the website or app (this connection to Facebook's servers occurs automatically when a person visits a website or app that contains our technologies, such as a Like button, and is an inherent function of Internet design); and (ii) any additional information the publisher of the app or website chooses to share with Facebook about the person's activities on that site (such as the fact that a purchase was made on the site). This is a standard feature of the Internet, and most websites and apps share this same information with multiple different third-parties whenever people visit their website or app. When the person visiting a website featuring Facebook's tools is not a registered Facebook user, Facebook does not have information identifying that individual, and it does not create profiles for this individual.

- We also may receive information about the device of a non-registered user if that user visits a part of Facebook that does not require people to log in—such as a public Facebook Page. The information we log when people visit our websites or apps is the

same as described above and is the same information that any provider of an online service would receive.

- In addition, Facebook may receive some basic information about devices where Facebook apps are installed, including before people using those devices have registered for Facebook (such as when a user downloads a Facebook app, but has not yet created an account, or if the app is preloaded on a given device). This device data includes things like device model, operating system, IP address, app version and device identifiers. We use this information to provide the right version of the app, help people who want to create accounts (for example, optimizing the registration flow for the specific device), retrieving bug fixes and measuring and improving app performance. We do not use this information to build profiles about non-registered users.

506. Why should we trust you?

Facebook's policies regarding third-party usage of its platform technologies have prohibited—and continue to prohibit—third-party app developers from selling or licensing user data obtained from Facebook and from sharing any user data obtained from Facebook with any ad network, data broker or other advertising or monetization-related service.

We use a variety of tools to enforce Facebook policies against violating parties, including developers. We review tens of thousands of apps per year and regularly disapprove noncompliant apps as part of our proactive review process. We also use tools like cease and desist letters, account suspensions, letter agreements, and civil litigation. For example, since 2006, Facebook has sent over 1,150 cease-and-desist letters to over 1,600 targets. In 2017, we took action against about 370,000 apps, ranging from imposing certain restrictions to removal of the app from the platform. Moreover, we have required parties who have procured our data without authorization to delete that data. We have invested significant resources in these efforts.

Recently, we announced a number of additional steps we're taking to address concerns raised by Kogan's app.

- **Review our platform.** We will investigate all apps that had access to large amounts of data before the platform changes we announced in 2014, and we will audit any app where we identify suspicious activity. If we identify misuses of data, we'll take immediate action, including banning the app from our platform and pursuing legal action if appropriate.

- **Tell people about data misuse.** We will tell people about apps that have misused their data. This includes building a way for people to know if their data might have been accessed via the app. Moving forward, if we remove an app, we will tell people.

- **Turn off access for unused apps.** If someone has not used an app within the last three months, we will turn off the app's access to their data.

- **Restrict Facebook Login data.** We are changing Login, so that the only data that an app can request without app review will include name, profile photo, and email

address. Requesting any other data will require approval from Facebook. We will also no longer allow apps to ask for access to information like religious or political views, relationship status and details, custom friends lists, education and work history, fitness activity, book reading and music listening activity, news reading, video watch activity, and games activity. We will encourage people to manage the apps they use. We already show people what apps their accounts are connected to and allow them to control what data they've permitted those apps to use. But we're making it easier for people to see what apps they use and the information they have shared with those apps.

- **Reward people who find vulnerabilities.** We launched the Data Abuse Bounty program so that people can report to us any misuses of data by app developers.

- **Update our policies.** We have updated our terms and Data Policy to explain how we use data and how data is shared with app developers.

507. For Anna: This certainly IS critically important! Why only 4 minutes/person?

As discussed with your staff, this question is not germane to the hearing.

508. Why shouldn't the same principle of truly informed consent (as in research) apply to fb?

We believe that it's important to communicate with people about the information that we collect and how people can control it. As explained in our Data Policy, we collect three basic categories of data about people:

(1) data about things people do and share (and who they connect with) on our services;

(2) data about the devices people use to access our services; and

(3) data we receive from partners, including the websites and apps that use our business tools.

We collect information about the people, Pages, accounts, hashtags, and groups users are connected to and how they interact with them across our Products, such as people a user communicates with the most or groups users are part of. We also collect contact information if they choose to upload, sync, or import it from a device (such as an address book or call log or SMS log history), which we use for things like helping them and others find people they may know.

The data we use to show ads to people depends on the data we have received from people. For people who are new to Facebook, we may have minimal data that we can use. For people who have used our services for longer, we likely have more data, but the amount of data will depend on the nature of that use and how they have used our controls. Any person can see each of the specific interests we maintain about them for advertising by visiting Ads Preferences, which lets people see what interests we use to choose ads for them—and to edit or delete these interests. We also provide more detailed information about how we use data to decide what ads

to show to people in our "About Facebook Ads" page, at https://www.facebook.com/ads/about. And, we do not sell people's information to anyone, and we never will.

All users must expressly consent to Facebook's Terms and Data Policy when registering for Facebook. The Data Policy explains the kinds of information we collect, how we use this information, how we share this information, and how users can manage and delete information.

Facebook does not create profiles for people without a Facebook account, but we do receive some information from devices and browsers that may be used by non-users. For example:

- When people visit apps or websites that feature our technologies—like the Facebook Like or Comment button—our servers automatically log (i) standard browser or app records of the fact that a particular device or user visited the website or app (this connection to Facebook's servers occurs automatically when a person visits a website or app that contains our technologies, such as a Like button, and is an inherent function of Internet design); and (ii) any additional information the publisher of the app or website chooses to share with Facebook about the person's activities on that site (such as the fact that a purchase was made on the site). This is a standard feature of the Internet, and most websites and apps share this same information with multiple different third-parties whenever people visit their website or app. When the person visiting a website featuring Facebook's tools is not a registered Facebook user, Facebook does not have information identifying that individual, and it does not create profiles for this individual.

- We also may receive information about the device of a non-registered user if that user visits a part of Facebook that does not require people to log in—such as a public Facebook Page. The information we log when people visit our websites or apps is the same as described above and is the same information that any provider of an online service would receive.

- In addition, Facebook may receive some basic information about devices where Facebook apps are installed, including before people using those devices have registered for Facebook (such as when a user downloads a Facebook app, but has not yet created an account, or if the app is preloaded on a given device). This device data includes things like device model, operating system, IP address, app version and device identifiers. We use this information to provide the right version of the app, help people who want to create accounts (for example, optimizing the registration flow for the specific device), retrieving bug fixes and measuring and improving app performance. We do not use this information to build profiles about non-registered users.

509. Russia, a historical US Ally must be able to assert our joint national security interests yet you disallow freedom of speech when it does not support Hillary Clinton whose husband former Pres Bill Clinton was Impeached nearly removed shy 1-2 votes in the US Senate for abuse of power and lying to FBI and Congress etc.

As discussed with your staff, this question is not germane to the hearing.

510. Please just let him know how transparently selfish & delusional he has shown himself to be. My privacy is MINE, not Facebook's to sell! How dare he ignore that?

As discussed with your staff, this question is not germane to the hearing.

511. I am praying for you.
Laurel Smith, Saratoga, CA

As discussed with your staff, this question is not germane to the hearing.

512. Comment to April 2, 2018 ACLU.org blog "Eight Questions Members of Congress Should Ask Mark Zuckerberg,": "Remember, Facebook users are the product, not the client." Facebook's business model is the processing and selling of member data, justified as a benefit to both users of the program and users of the data. Question: is it possible to envision a purely member centric model for Facebook and what would that look like compared to what it is now?

We believe that it's important to communicate with people about the information that we collect and how people can control it. As explained in our Data Policy, we collect three basic categories of data about people:

(1) data about things people do and share (and who they connect with) on our services;

(2) data about the devices people use to access our services; and

(3) data we receive from partners, including the websites and apps that use our business tools.

We collect information about the people, Pages, accounts, hashtags, and groups users are connected to and how they interact with them across our Products, such as people a user communicates with the most or groups users are part of. We also collect contact information if they choose to upload, sync, or import it from a device (such as an address book or call log or SMS log history), which we use for things like helping them and others find people they may know.

The data we use to show ads to people depends on the data we have received from people. For people who are new to Facebook, we may have minimal data that we can use. For people who have used our services for longer, we likely have more data, but the amount of data will depend on the nature of that use and how they have used our controls. Any person can see each of the specific interests we maintain about them for advertising by visiting Ads Preferences, which lets people see what interests we use to choose ads for them—and to edit or delete these interests. We also provide more detailed information about how we use data to decide what ads to show to people in our "About Facebook Ads" page, at https://www.facebook.com/ads/about. And, we do not sell people's information to anyone, and we never will.

All users must expressly consent to Facebook's Terms and Data Policy when registering for Facebook. The Data Policy explains the kinds of information we collect, how we use this information, how we share this information, and how users can manage and delete information.

Facebook does not create profiles for people without a Facebook account, but we do receive some information from devices and browsers that may be used by non-users. For example:

- When people visit apps or websites that feature our technologies—like the Facebook Like or Comment button—our servers automatically log (i) standard browser or app records of the fact that a particular device or user visited the website or app (this connection to Facebook's servers occurs automatically when a person visits a website or app that contains our technologies, such as a Like button, and is an inherent function of Internet design); and (ii) any additional information the publisher of the app or website chooses to share with Facebook about the person's activities on that site (such as the fact that a purchase was made on the site). This is a standard feature of the Internet, and most websites and apps share this same information with multiple different third-parties whenever people visit their website or app. When the person visiting a website featuring Facebook's tools is not a registered Facebook user, Facebook does not have information identifying that individual, and it does not create profiles for this individual.

- We also may receive information about the device of a non-registered user if that user visits a part of Facebook that does not require people to log in—such as a public Facebook Page. The information we log when people visit our websites or apps is the same as described above and is the same information that any provider of an online service would receive.

- In addition, Facebook may receive some basic information about devices where Facebook apps are installed, including before people using those devices have registered for Facebook (such as when a user downloads a Facebook app, but has not yet created an account, or if the app is preloaded on a given device). This device data includes things like device model, operating system, IP address, app version and device identifiers. We use this information to provide the right version of the app, help people who want to create accounts (for example, optimizing the registration flow for the specific device), retrieving bug fixes and measuring and improving app performance. We do not use this information to build profiles about non-registered users.

513. What do you consider the biggest danger to your real users and what are you doing to protect them.

We believe everyone deserves good privacy controls. A user owns the information they share on Facebook. This means they decide what they share and who they share it with on Facebook, and they can change their mind. We require websites and apps who use our tools to tell users they're collecting and sharing their information with us, and to get users' permission to do so.

Everyone has the right to expect strong protections for their information. We also need to do our part to help keep our community safe, in a way that's consistent with people's privacy expectations. We've recently announced several steps to give people more control over their privacy, including a new Privacy Shortcuts tool that we're rolling out now to give people information about how to control their information, including choosing who can see what they

post and adding protections like two-factor authentication to their account. People can learn more about how to protect their privacy in our updated Data Policy and in our Privacy Basics feature (https://www.facebook.com/about/basics).

We are in the process of investigating every app that had access to a large amount of information before we changed our Platform in 2014. The investigation process is in full swing. We have large teams of internal and external experts working hard to investigate these apps as quickly as possible. As of early June 2018, thousands of apps have been investigated and around 200 apps have been suspended—pending a thorough investigation into whether they did in fact misuse any data. Where we find evidence that these or other apps did misuse data, we will ban them and let people know.

Facebook is generally not opposed to regulation but wants to ensure it is the right regulation. The issues facing the industry are complex, multi-faceted, and affect an important part of peoples' lives. As such, Facebook is absolutely committed to working with regulators, like Congress, to craft the right regulations. Facebook would be happy to review any proposed legislation and provide comments.

514. Two family members work for you and believed in your goodness. How will you answer to them?

We recognize that we have made mistakes, and we are committed to learning from this experience to secure our platform further and make our community safer for everyone going forward. As our CEO Mark Zuckerberg has said, when you are building something unprecedented like Facebook, there are going to be mistakes. What people should hold us accountable for is learning from the mistakes and continually doing better—and, at the end of the day, making sure that we're building things that people like and that make their lives better.

Particularly in the past few months, we've realized that we need to take a broader view of our responsibility to our community. Part of that effort is continuing our ongoing efforts to identify ways that we can improve our privacy practices. We've heard loud and clear that privacy settings and other important tools are too hard to find and that we must do more to keep people informed. So, we're taking additional steps to put people more in control of their privacy. For instance, we redesigned our entire settings menu on mobile devices from top to bottom to make things easier to find. We also created a new Privacy Shortcuts in a menu where users can control their data in just a few taps, with clearer explanations of how our controls work. The experience is now clearer, more visual, and easy-to-find. Furthermore, we also updated our terms of service that include our commitments to everyone using Facebook. We explain the services we offer in language that's easier to read. We've also updated our Data Policy to better spell out what data we collect and how we use it in Facebook, Instagram, Messenger, and other products.

515. Please ask Mr. Zuckerberg if the rumors for many years are true concerning the CIA having complete access to our Facebook accounts. Thank you, Mark Schwenne

We believe everyone deserves good privacy controls. A user owns the information they share on Facebook. This means they decide what they share and who they share it with on Facebook, and they can change their mind. We require websites and apps who use our tools to

tell users they're collecting and sharing their information with us, and to get users' permission to do so.

Everyone has the right to expect strong protections for their information. We also need to do our part to help keep our community safe, in a way that's consistent with people's privacy expectations. We've recently announced several steps to give people more control over their privacy, including a new Privacy Shortcuts tool that we're rolling out now to give people information about how to control their information, including choosing who can see what they post and adding protections like two-factor authentication to their account. People can learn more about how to protect their privacy in our updated Data Policy and in our Privacy Basics feature (https://www.facebook.com/about/basics).

We are in the process of investigating every app that had access to a large amount of information before we changed our Platform in 2014. The investigation process is in full swing. We have large teams of internal and external experts working hard to investigate these apps as quickly as possible. As of early June 2018, thousands of apps have been investigated and around 200 apps have been suspended—pending a thorough investigation into whether they did in fact misuse any data. Where we find evidence that these or other apps did misuse data, we will ban them and let people know.

Facebook is generally not opposed to regulation but wants to ensure it is the right regulation. The issues facing the industry are complex, multi-faceted, and affect an important part of peoples' lives. As such, Facebook is absolutely committed to working with regulators, like Congress, to craft the right regulations. Facebook would be happy to review any proposed legislation and provide comments.

516. Did he vote for Trump?

As discussed with your staff, this question is not germane to the hearing.

517. How often do u change your tee shirt and do you plan to wear appropriate dress before the committee?

As discussed with your staff, this question is not germane to the hearing.

518. Does Facebook have to concentrate all their employees in Menlo Park? Spread the joy!

As discussed with your staff, this question is not germane to the hearing.

519. Does your board want you to resign? Not addressing security is armature behavior?

We recognize that we have made mistakes, and we are committed to learning from this experience to secure our platform further and make our community safer for everyone going forward. As our CEO Mark Zuckerberg has said, when you are building something unprecedented like Facebook, there are going to be mistakes. What people should hold us accountable for is learning from the mistakes and continually doing better—and, at the end of the day, making sure that we're building things that people like and that make their lives better.

Particularly in the past few months, we've realized that we need to take a broader view of our responsibility to our community. Part of that effort is continuing our ongoing efforts to identify ways that we can improve our privacy practices. We've heard loud and clear that privacy settings and other important tools are too hard to find and that we must do more to keep people informed. So, we're taking additional steps to put people more in control of their privacy. For instance, we redesigned our entire settings menu on mobile devices from top to bottom to make things easier to find. We also created a new Privacy Shortcuts in a menu where users can control their data in just a few taps, with clearer explanations of how our controls work. The experience is now clearer, more visual, and easy-to-find. Furthermore, we also updated our terms of service that include our commitments to everyone using Facebook. We explain the services we offer in language that's easier to read. We've also updated our Data Policy to better spell out what data we collect and how we use it in Facebook, Instagram, Messenger, and other products.

520. Please forward to the Congresswoman my suggestion --for her to formulate into a question- to seek from Mr. Zuckerberg and Facebook the commitment—including periodic progress reports of this commitment— to use the Facebook platform to cultivate users to become immunized of the credulity of artificial news. It is more important call out Facebook to step up to the plate to help our democratic process and culture to countervail the bad actors who try to weaken or disrupt it, than it is to let Mr. Zuckerberg and friends retreat to the obfuscation of their technology.

We want Facebook to be a place where people can discover more news, information, and perspectives, and we are working to build products that help to that. Through our News Feed algorithm, we also work hard to actively reduce the distribution of clickbait, sensationalism, and misinformation, on the one hand, and to boost news and information from sources that are trusted, informative, and local, on the other hand.

We are focusing on four different strategies to address misinformation:

- **Strengthening enforcement of our authenticity policies.** We are investing heavily in new technology and hiring thousands more people to tackle the problem of inauthenticity on the platform. Fake accounts are often associated with false news, so this is an area that will have a huge impact on curbing the spread of inaccurate information.

- **Finding industry solutions.** All of us—from tech companies and media companies to newsrooms and classrooms—must work together to find industry solutions to strengthen the online news ecosystem and our own digital literacy. That's why we're collaborating with others who operate in this space. Last January, we announced The Facebook Journalism Project, an initiative that seeks to establish stronger ties between Facebook and the news industry. The project is focused on developing news products, providing training and tools for journalists, and working with publishers and educators on how we can equip people with the knowledge they need to be informed readers in the digital age. Since launching the Journalism Project, we've met with more than 2,600 publishers around the world to understand how they use our products and how we can make improvements to better support their needs.

- **Disrupting economic incentives.** When it comes to fighting false news, we've found that a lot of it is financially motivated. So, one of the most effective approaches is removing the economic incentives for those who traffic in inaccurate information. We've done things like block ads from pages that repeatedly share false news and significantly limit the distribution of web pages that deliver low quality web experiences.

- **Building new products.** We believe it's important to amplify the good effects of social media and mitigate the bad—to contribute to the diversity of ideas, information, and view points, while strengthening our common understanding.

    - We believe giving people more context can help them decide what to trust and what to share. The third-party fact-checking program we have developed uses reports from our community, along with other signals, to send stories to accredited third-party fact checking organizations. If the fact checking organizations identify a story as fake, we will suggest related articles in News Feed to show people different points of view, including information from fact checkers. Stories that have been disputed may also appear lower in News Feed. Our own data analytics show that a false rating from one of our fact checking partners reduces future impressions on Facebook by 80 percent.

    - We're also testing Article Context as a way of giving people more information about the material they're reading on Facebook. Since we launched this test, some of the articles people see in News Feed will feature an "i" icon that allows them to access more information at the tap of a button. The information we surface is pulled from across the internet, and includes things like the publisher's Wikipedia entry, trending articles or related articles about the topic, and information about how the article is being shared on Facebook. In some cases, if that information is unavailable, we will let people know since that can also be helpful context.

521. Do you see the danger of this trend continuing with home assistance devices?

We believe everyone deserves good privacy controls. A user owns the information they share on Facebook. This means they decide what they share and who they share it with on Facebook, and they can change their mind. We require websites and apps who use our tools to tell users they're collecting and sharing their information with us, and to get users' permission to do so.

Everyone has the right to expect strong protections for their information. We also need to do our part to help keep our community safe, in a way that's consistent with people's privacy expectations. We've recently announced several steps to give people more control over their privacy, including a new Privacy Shortcuts tool that we're rolling out now to give people information about how to control their information, including choosing who can see what they post and adding protections like two-factor authentication to their account. People can learn more about how to protect their privacy in our updated Data Policy and in our Privacy Basics feature (https://www.facebook.com/about/basics).

We are in the process of investigating every app that had access to a large amount of information before we changed our Platform in 2014. The investigation process is in full swing. We have large teams of internal and external experts working hard to investigate these apps as quickly as possible. As of early June 2018, thousands of apps have been investigated and around 200 apps have been suspended—pending a thorough investigation into whether they did in fact misuse any data. Where we find evidence that these or other apps did misuse data, we will ban them and let people know.

Facebook is generally not opposed to regulation but wants to ensure it is the right regulation. The issues facing the industry are complex, multi-faceted, and affect an important part of peoples' lives. As such, Facebook is absolutely committed to working with regulators, like Congress, to craft the right regulations. Facebook would be happy to review any proposed legislation and provide comments.

522. Thanks for employing so many people, what are your expansion plans

We recognize that we have made mistakes, and we are committed to learning from this experience to secure our platform further and make our community safer for everyone going forward. As our CEO Mark Zuckerberg has said, when you are building something unprecedented like Facebook, there are going to be mistakes. What people should hold us accountable for is learning from the mistakes and continually doing better—and, at the end of the day, making sure that we're building things that people like and that make their lives better.

Particularly in the past few months, we've realized that we need to take a broader view of our responsibility to our community. Part of that effort is continuing our ongoing efforts to identify ways that we can improve our privacy practices. We've heard loud and clear that privacy settings and other important tools are too hard to find and that we must do more to keep people informed. So, we're taking additional steps to put people more in control of their privacy. For instance, we redesigned our entire settings menu on mobile devices from top to bottom to make things easier to find. We also created a new Privacy Shortcuts in a menu where users can control their data in just a few taps, with clearer explanations of how our controls work. The experience is now clearer, more visual, and easy-to-find. Furthermore, we also updated our terms of service that include our commitments to everyone using Facebook. We explain the services we offer in language that's easier to read. We've also updated our Data Policy to better spell out what data we collect and how we use it in Facebook, Instagram, Messenger, and other products.

523. How can we stop invisible Individually-targeted propaganda machines that seek to alter election results?

We want Facebook to be a place where people can discover more news, information, and perspectives, and we are working to build products that help to that. Through our News Feed algorithm, we also work hard to actively reduce the distribution of clickbait, sensationalism, and misinformation, on the one hand, and to boost news and information from sources that are trusted, informative, and local, on the other hand.

We are focusing on four different strategies to address misinformation:

- **Strengthening enforcement of our authenticity policies.** We are investing heavily in new technology and hiring thousands more people to tackle the problem of inauthenticity on the platform. Fake accounts are often associated with false news, so this is an area that will have a huge impact on curbing the spread of inaccurate information.

- **Finding industry solutions.** All of us—from tech companies and media companies to newsrooms and classrooms—must work together to find industry solutions to strengthen the online news ecosystem and our own digital literacy. That's why we're collaborating with others who operate in this space. Last January, we announced The Facebook Journalism Project, an initiative that seeks to establish stronger ties between Facebook and the news industry. The project is focused on developing news products, providing training and tools for journalists, and working with publishers and educators on how we can equip people with the knowledge they need to be informed readers in the digital age. Since launching the Journalism Project, we've met with more than 2,600 publishers around the world to understand how they use our products and how we can make improvements to better support their needs.

- **Disrupting economic incentives.** When it comes to fighting false news, we've found that a lot of it is financially motivated. So, one of the most effective approaches is removing the economic incentives for those who traffic in inaccurate information. We've done things like block ads from pages that repeatedly share false news and significantly limit the distribution of web pages that deliver low quality web experiences.

- **Building new products.** We believe it's important to amplify the good effects of social media and mitigate the bad—to contribute to the diversity of ideas, information, and view points, while strengthening our common understanding.

    - We believe giving people more context can help them decide what to trust and what to share. The third-party fact-checking program we have developed uses reports from our community, along with other signals, to send stories to accredited third-party fact checking organizations. If the fact checking organizations identify a story as fake, we will suggest related articles in News Feed to show people different points of view, including information from fact checkers. Stories that have been disputed may also appear lower in News Feed. Our own data analytics show that a false rating from one of our fact checking partners reduces future impressions on Facebook by 80 percent.

    - We're also testing Article Context as a way of giving people more information about the material they're reading on Facebook. Since we launched this test, some of the articles people see in News Feed will feature an "i" icon that allows them to access more information at the tap of a button. The information we surface is pulled from across the internet, and includes things like the publisher's Wikipedia entry, trending articles or related articles about the topic, and information about how the article is being shared on Facebook. In some cases, if that information is unavailable, we will let people know since that can also be helpful context.

524. The Menlo Park Police Department are getting calls from Facebook customers who are frustrated that they can't get through to Facebook to answer their questions, delete their account. Could you Mr. Z tell me about your customer interface and how your Facebook users can get their answers answered directly...not digitally?

As discussed with your staff, this question is not germane to the hearing.

The Honorable Eliot Engel

1. Your testimony to our Committee referenced "networks of fake accounts" established by Russian entities to target American citizens and interfere in the 2016 U.S. presidential election. Will you please describe the tools and tactics used by Russian entities to execute information operations against American citizens, and detail the narratives they pursued?

In the run-up to the 2016 elections, we were focused on the kinds of cybersecurity attacks typically used by nation states, for example phishing and malware attacks.

We learned from press accounts and statements by congressional leaders that Russian actors might have tried to interfere in the 2016 election by exploiting Facebook's ad tools. This is not something we had seen before, and so we started an investigation. We found that fake accounts associated with the IRA spent approximately $100,000 on around 3,500 Facebook and Instagram ads between June 2015 and August 2017. Our analysis also showed that these accounts used these ads to promote the roughly 120 Facebook Pages they had set up, which in turn posted more than 80,000 pieces of content between January 2015 and August 2017. The Facebook accounts that appeared tied to the IRA violated our policies because they came from a set of coordinated, inauthentic accounts. We shut these accounts down and began trying to understand how they misused our platform. We shared the ads we discovered with Congress, in a manner that is consistent with our obligations to protect user information, to help government authorities complete the vitally important work of assessing what happened in the 2016 election. The ads (along with the targeting information) are publicly available at https://democrats-intelligence.house.gov/facebook-ads/social-media-advertisements.htm.

We have used the best tools and analytical techniques that are available to us to identify the full extent of this malicious activity, and we continue to monitor our platform for abuse and to share and receive information from others in our industry about these threats.

2. You testified that Facebook "should have spotted Russian interference earlier," and that Facebook is "working hard to make sure it doesn't happen again." You then cited new technologies that Facebook has built and subsequently deployed to protect French and German democracies in 2017, and that were also deployed in the U.S. Senate special election in Alabama. Will Facebook extend those same protections to the entire United States? To all democracies across the globe? What is your timeline?

Over the past year, we've gotten increasingly better at finding and disabling fake accounts. We now block millions of fake accounts each day as people try to create them—and before they've done any harm. This is thanks to improvements in machine learning and artificial intelligence, which can proactively identify suspicious behavior at a scale that was not possible before—without needing to look at the content itself.

In recent months, we've started to deploy new tools and teams to proactively identify threats in the run-up to specific elections. We first tested this effort during the Alabama Senate election, and plan to continue these efforts for elections around the globe, including the US

midterms. Last year we used public service announcements to help inform people about fake news in 21 separate countries, including in advance of French, Kenyan and German elections.

3. Various media outlets have reported that the Russian government requires companies like Facebook to store their data in Russia. What personal data does Facebook make available to the Russian state media monitoring agency Roskomnadzor or other Russian agencies? Does this apply only to accounts located in or operated from Russia, or does this also include Facebook's global data? Will you agree to share this data with the United States government?

As part of our ongoing effort to share information about the requests we have received from governments around the world, Facebook regularly produces a Transparency Report about government data requests to Facebook. Our Transparency Report contains historical information about Russian requests for data going back to 2013. In summary, we received 34 requests from the Russian government between 2013 and 2017. We did not provide any data in response to these requests. See https://transparency.facebook.com/government-data-requests/country/RU.

4. Did Facebook preserve all of the data and content connected to Russian information operations conducted against American citizens? If so, will Facebook make that data and content available to researchers or intelligence agencies for evaluation?

Facebook has taken appropriate steps to retain relevant information related to IRA activity on Facebook.

Facebook has conducted a broad search for evidence that Russian actors, not limited to the IRA or any other specific entity or organization, attempted to interfere in the 2016 election by using Facebook's advertising tools. We found coordinated activity that we now attribute to the IRA, despite efforts by these accounts to mask the provenance of their activity. We have used the best tools and analytical techniques that are available to us to identify the full extent of this malicious activity, and we continue to monitor our platform for abuse and to share and receive information from others in our industry about these threats.

We will continue to work with the government, and across the tech industry and civil society, to address this important national security matter so that we can do our part to prevent similar abuse from happening again. That's why we have provided all of the ads and associated information to the committees with longstanding, bipartisan investigations into Russian interference, and we defer to the committees to share as appropriate. We believe that Congress and law enforcement are best positioned to assess the nature and intent of these activities.

5. What assistance do Facebook employees embedded with advertising clients provide? Did any Facebook employees provide support to the Internet Research Agency or any other business or agency in Russia targeting content to American citizens?

No Facebook employee was embedded with the Internet Research Agency, and they were never supported as a managed advertiser. The targeting for the IRA ads that we have identified and provided to the Committee was relatively rudimentary, targeting very broad locations and interests. For example, the targeting for IRA ads only used custom audiences in a very small percentage of its overall targeting and did not use Contact List Custom Audiences. In addition,

all of the custom audiences used by the IRA were created based on user engagement with certain IRA pages.

6. As part of Facebook's "custom audiences" feature, entities can upload datasets to target Facebook users. Does Facebook have copies of data uploaded to "custom audiences" by any Russian entity? If so, will Facebook make that data and content available to researchers or intelligence agencies for evaluation?

See Response to Question 4.

7. You referred to Chinese internet companies as a "strategic and technological threat." Will you please elaborate? Explain which Chinese companies you're referencing, what they are doing, and how this is similar to or different from activities of the Russians?

This reference alludes to the fast-growing prominence of Chinese internet companies and that unless American companies can innovate, there is a risk of falling behind Chinese competitors and others around the world. Venture capitalist Mary Meeker recently prepared a report detailing internet trends, including the growth of Chinese internet companies, available at http://www.kpcb.com/internet-trends.

The threat that we are referring to here is a competitive threat which is different from that posed by the activities of the Internet Research Agency.

8. Has Facebook performed any internal research or evaluation of these tools and tactics used by Russian entities to execute information operations against American citizens? Or about how the psychological impacts of these operations can be mitigated? Would you consider trying to mitigate the damage of disinformation campaigns on Facebook by prominently notifying individual users every time they have viewed (not just shared, but viewed) fake, malicious, or disinformation campaign content?

In the run-up to the 2016 elections, we were focused on the kinds of cybersecurity attacks typically used by nation states, for example phishing and malware attacks. And we were too slow to spot this type of information operations interference. Since then, we've made important changes to prevent bad actors from using misinformation to undermine the democratic process.

This will never be a solved problem because we're up against determined, creative, and well-funded adversaries. But we are making steady progress. Here is a list of the 10 most important changes we have made:

- **Ads transparency.** Advertising should be transparent: users should be able to see all the ads an advertiser is currently running on Facebook, Instagram and Messenger. And for ads with political content, we've created an archive that will hold ads with political content for seven years—including information about ad impressions and spend, as well as demographic data such as age, gender, and location. People in

Canada and Ireland have already been able to see all the ads that a Page is running on Facebook—and we've launched this globally.

- **Verification and labeling.** Every advertiser will now need to confirm their ID and location before being able to run any ads with political content in the US. All ads with political content will also clearly state who paid for them.

- **Updating targeting.** We want ads on Facebook to be safe and civil. We thoroughly review the targeting criteria advertisers can use to ensure they are consistent with our principles. As a result, we removed nearly one-third of the targeting segments used by the IRA. We continue to allow some criteria that people may find controversial. But we do see businesses marketing things like historical books, documentaries or television shows using them in legitimate ways.

- **Better technology.** Over the past year, we've gotten increasingly better at finding and disabling fake accounts. We now block millions of fake accounts each day as people try to create them—and before they've done any harm. This is thanks to improvements in machine learning and artificial intelligence, which can proactively identify suspicious behavior at a scale that was not possible before—without needing to look at the content itself.

- **Action to tackle fake news.** We block millions of fake account attempts each day as people try to create them thanks to improvements in machine learning and artificial intelligence. We are also working hard to stop the spread of false news. To reduce the spread of false news, we remove fake accounts and disrupt economic incentives for traffickers of misinformation. We also use various signals, including feedback from our community, to identify potential false news. In countries where we have partnerships with independent third-party fact-checkers, stories rated as false by those fact-checkers are shown lower in News Feed. If Pages or domains repeatedly create or share misinformation, we significantly reduce their distribution and remove their advertising rights.

- **Significant investments in security.** We're doubling the number of people working on safety and security from 10,000 last year to over 20,000 this year. We expect these investments to impact our profitability. But the safety of people using Facebook needs to come before profit.

- **Industry collaboration.** Recently, we joined 34 global tech and security companies in signing a TechAccord pact to help improve security for everyone.

- **Information sharing and reporting channels.** In the 2017 German elections, we worked closely with the authorities there, including the Federal Office for Information Security (BSI). This gave them a dedicated reporting channel for security issues related to the federal elections.

- **Tracking 40+ elections.** In recent months, we've started to deploy new tools and teams to proactively identify threats in the run-up to specific elections. We first tested

this effort during the Alabama Senate election, and plan to continue these efforts for elections around the globe, including the US midterms. Last year we used public service announcements to help inform people about fake news in 21 separate countries, including in advance of French, Kenyan and German elections.

- **Action against the Russia-based IRA.** In April, we removed 70 Facebook and 65 Instagram accounts—as well as 138 Facebook Pages—controlled by the IRA primarily targeted either at people living in Russia or Russian-speakers around the world including from neighboring countries like Azerbaijan, Uzbekistan, and Ukraine. The IRA has repeatedly used complex networks of inauthentic accounts to deceive and manipulate people in the US, Europe and Russia—and we don't want them on Facebook anywhere in the world.

We are taking steps to enhance trust in the authenticity of activity on our platform, including increasing ads transparency, implementing a more robust ads review process, imposing tighter content restrictions, and exploring how to add additional authenticity safeguards.

We are working to build a more informed community by promoting trustworthy, informative, and local news and by focusing on four different strategies to address misinformation:

- Strengthening enforcement of our authenticity policies. We are investing heavily in new technology and hiring thousands more people to tackle the problem of inauthenticity on the platform. Fake accounts are often associated with false news, so this is an area that will have a huge impact on curbing the spread of inaccurate information.

- Finding industry solutions. All of us—from tech companies and media companies to newsrooms and classrooms—must work together to find industry solutions to strengthen the online news ecosystem and our own digital literacy. That's why we're collaborating with others who operate in this space. Last January, we announced The Facebook Journalism Project, an initiative that seeks to establish stronger ties between Facebook and the news industry. The project is focused on developing news products, providing training and tools for journalists, and working with publishers and educators on how we can equip people with the knowledge they need to be informed readers in the digital age. Since launching the Journalism Project, we've met with more than 2,600 publishers around the world to understand how they use our products and how we can make improvements to better support their needs.

- Disrupting economic incentives. When it comes to fighting false news, we've found that a lot of it is financially motivated. So, one of the most effective approaches is removing the economic incentives for those who traffic in inaccurate information. We've done things like block ads from pages that repeatedly share false news and significantly limit the distribution of web pages that deliver low quality web experiences.

- Building new products. We believe it's important to amplify the good effects of social media and mitigate the bad—to contribute to the diversity of ideas, information, and view points, while strengthening our common understanding.

We believe giving people more context can help them decide what to trust and what to share. The third-party fact-checking program we have developed uses reports from our community, along with other signals, to send stories to accredited third-party fact checking organizations. If the fact-checking organizations identify a story as fake, we will suggest related articles in News Feed to show people different points of view, including information from fact checkers. Stories that have been disputed may also appear lower in News Feed. Our own data analytics show that a false rating from one of our fact checking partners reduces future impressions on Facebook by 80 percent.

We're also testing Article Context as a way of giving people more information about the material they're reading on Facebook. Since we launched this test, some of the articles people see in News Feed will feature an "i" icon that allows them to access more information at the tap of a button. The information we surface is pulled from across the internet, and includes things like the publisher's Wikipedia entry, trending articles or related articles about the topic, and information about how the article is being shared on Facebook. In some cases, if that information is unavailable, we will let people know since that can also be helpful context.

9. One of the things that I raised during our hearing was the role of social platforms in the ethnic cleansing in Burma, which resulted in the second largest refugee crisis in the world. I understand that Facebook has taken steps in six countries to work with independent third parties to intensify fact checking efforts, and that fact-checkers report that it typically takes three days to correct a false article in these countries. Do you intend to help expand fact checking capacity to service the full range of languages and countries that Facebook operates in, and do you aim to improve the time it takes to issue corrections? On what timeline?

We are investing in people, technology, and programs to help address the very serious challenges we have seen in places like Myanmar and Sri Lanka.

Our content review teams around the world—which grew by 3,000 people last year—work 24 hours a day and in over 50 languages.

Our goal is always to have the right number of people with the right native language capabilities to ensure incoming reports are reviewed quickly and effectively. That said, there is more to tackling this problem than reported content. A lot of abuse may go unreported, which is why we are supplementing our hiring with investments in technology and programs.

We are building new tools so that we can more quickly and effectively detect abusive, hateful, or false content. We have, for example, designated several hate figures and organizations for repeatedly violating our hate speech policies, which has led to the removal of accounts and content that support, praise, or represent these individuals or organizations. We are also investing in artificial intelligence that will help us improve our understanding of dangerous content.

From a programmatic perspective, we will continue to work with experts to develop safety resources and counter-speech campaigns in these regions and conduct regular training for civil society and community groups on using our tools.

10. I'm interested in learning about Facebook's efforts to track disinformation campaigns, including efforts to track patterns of fake account and bot activity. What can you tell me about the scope and scale of these campaigns on Facebook right now? Going forward, will you commit to regular full disclosure of the extent of fake users, fake activity, and disinformation campaigns on your platform?

Stopping the abuse of fake accounts and malicious bot activity is a focus for many teams, some more directly and some in more of a supportive role. For example, we are expanding our threat intelligence team, and more broadly, we are working now to ensure that we will more than double the number of people working on safety and security at Facebook, from 10,000 to 20,000, by the end of 2018. We expect to have at least 250 people specifically dedicated to safeguarding election integrity on our platforms, and that number does not include the thousands of people who will contribute to this effort in some capacity. Many of the people we are adding to these efforts will join our ad review team, and we also expect to add at least 3,000 people to Community Operations, which reviews content that our users and automated tools flag as inappropriate, dangerous, abusive, or otherwise violating our policies. We also continue to make improvements to our efforts to more effectively detect and deactivate fake accounts to help reduce the spread of spam, false news, and misinformation. We continually update our technical systems to identify, checkpoint, and remove inauthentic accounts, and we block millions of attempts to register fake accounts every day. These systems examine thousands of detailed account attributes and prioritize signals that are more difficult for bad actors to disguise, such as their connections to others on our platform. As with all security threats, we have been incorporating new insights into our models for detecting fake accounts, including information specific to election issues.

We publish information and metrics about fake accounts at https://transparency.facebook.com/community-standards-enforcement#fake-accounts and in our quarterly SEC filings.

The Honorable Gene Green

1. **In the April 11 hearing before the Energy & Commerce Committee, several members asked for assurances that Facebook would extend the exact same protections, rather than the same controls, to Americans as those that will be extended to EU citizens under the GDPR. Mr. Zuckerberg declined to give a yes or no answer. Can Facebook assure this committee that Americans will see identical permission screens, with the same prompts and asking for the same permissions, at the same points in the process of signing up for and using Facebook?**

As a part of our overall approach to privacy, we are providing the same tools for access, rectification, erasure, data portability and others to people in the US (and globally) that we provide in the European Union under the GDPR. The controls and settings that Facebook is enabling as part of GDPR include settings for controlling our use of face recognition on Facebook and for controlling our ability to use data we collect off Facebook Company Products to target ads. We recently began providing direct notice of these controls and our updated terms to people around the world (including in the US), allowing people to choose whether or not to enable or disable these settings or to consent to our updated terms. Many of these tools (like our Download Your Information tool, ad preferences tool, and Activity Log) have been available globally for many years.

The substantive protections in our user agreements offered by Facebook Ireland and Facebook, Inc. are the same. However, there are certain aspects of our Facebook Ireland Data Policy that are specific to legal requirements in the GDPR—such as the requirement that we provide contact information for our EU Data Protection Officer or that we identify the "legal bases" we use for processing data under the GDPR. Likewise, our Facebook Ireland terms and Data Policy address the lawful basis for transferring data outside the EU, based on legal instruments that are applicable only to the EU. And other provisions of the GDPR itself pertain to interactions between European regulators and other matters that are not relevant to people located outside of the EU.

Facebook is subject to ongoing oversight by the Federal Trade Commission with respect to its privacy commitments to people and its implementation of privacy settings, under a Consent Order with the FTC. Facebook is subject to the authority of the Irish Data Protection Commissioner, its lead regulator, under the GDPR in the European Union.

We are seeking explicit consent from people in Europe to three specific uses of data: facial recognition data (which previously was not enabled in Europe), special categories of data, and use of data we collect off Facebook Company Products to target ads. As noted above, we recently began providing direct notice of these controls and our updated terms to people around the world (including in the US), allowing people to choose whether or not to enable or disable these settings or to agree to our updated terms. Outside of Europe we are not requiring people to complete those flows if they repeatedly indicate that they do not want to go through the experience. At the same time, the events of recent months have underscored how important it is to make sure people know how their information is used and what their choices are. So, we decided to communicate prominently on Facebook—through a full-screen message and a

reminder to review at a later date. People can choose to dismiss or ignore these messages and continue using Facebook.

GDPR does not require consent for most uses of personal information, and instead, recognizes that many uses of data are necessary to provide a service or within companies' legitimate interests or the public interest. We agree that different levels of consent or notice are appropriate depending on the type of information or contemplated use at issue.

The Honorable Diana DeGette

1. **What are the future plans for making sure that all democratic elections in the world are not altered, or destroyed, by Facebook bad players, i.e., criminals masquerading as academics? How can they help stop the hateful, verbal, bullying going on? Criminal threats should not be allowed, and should be prosecuted; could they help? Please also thank him for allowing us all to connect worldwide, and share our views, opinions, inspirations, help, assistance, fun and funny items too!**

We recently outlined steps we are taking on election integrity here: https://newsroom.fb.com/news/2018/03/hard-questions-election-security/.

Further, pursuant to the new transparency measures Facebook is launching, all advertisers who want to run ads with political content targeted at the US will have to confirm their identity and location by providing either a US driver's license or passport, last four digits of their social security number, and a residential mailing address. Ads that include political content and appear on Facebook or Instagram will include a "Paid for by" disclaimer provided by the advertisers that shows the name of the funding source for the ad.

2. **How would Mr. Zuckerberg encourage people using Facebook to take some personal responsibility in checking for sources of postings?**

To reduce the spread of false news, one of the things we're doing is working with third-party fact checkers to let people know when they are sharing news stories (excluding satire and opinion) that have been disputed or debunked, and to limit the distribution of stories that have been flagged as misleading, sensational, or spammy. Third-party fact-checkers on Facebook are signatories to the non-partisan International Fact-Checking Network Code of Principles. Third-party fact-checkers investigate stories in a journalistic process meant to result in establishing the truth or falsity of the story.

In the United States, Facebook uses third-party fact-checking by the Associated Press, Factcheck.org, PolitiFact, Snopes, and the Weekly Standard Fact Check. Publishers may reach out directly to the third-party fact-checking organizations if (1) they have corrected the rated content, or if (2) they believe the fact-checker's rating is inaccurate. To issue a correction, the publisher must correct the false content and clearly state that a correction was made directly on the story. To dispute a rating, the publisher must clearly indicate why the original rating was inaccurate. If a rating is successfully corrected or disputed, the demotion on the content will be lifted and the strike against the domain or Page will be removed. It may take a few days to see the distribution for the domain or Page recover. Additionally, any recovery will be affected by other false news strikes and related interventions (like demotions for clickbait). Corrections and disputes are processed at the fact-checker's discretion. Fact-checkers are asked to respond to requests in a reasonable time period—ideally one business day for a simple correction, and up to a few business days for more complex disputes.

We want Facebook to be a place where people can discover more news, information, and perspectives, and we are working to build products that help.

3. In Europe, Facebook had to hire "hundreds" of additional staff and implement new procedures to ensure that hate speech and "fake news" were removed from the site in a timely manner. Why, after admitting that both of these are currently issues on Facebook in the US, is Facebook not devoting the same resources, proportionately, to tackling the problem here? I'm wondering if they will only do this in countries where they are legally required to, and continue to take zero responsibility in countries where they're not.

Our effort to make our platform safer and more secure is a holistic one that involves a continual evaluation of our personnel, processes, and policies, and we make changes as appropriate.

We are doubling the size of our security and content review teams (from 10,000 to 20,000) over the course of this year. We currently have approximately 15,000 people working on these teams. Of that 15,000, more than 7,500 people review content around the world.

- Our content review team is global and reviews reports in over 50 languages.
- Reports are reviewed 24 hours a day, 7 days a week and the vast majority of reports are reviewed within 24 hours.
- Our goal is always to have the right number of skilled people with the right language capabilities to ensure incoming reports are reviewed quickly and efficiently.
- We hire people with native language and other specialist skills according to the needs we see from incoming reports.
- The team also includes specialists in areas like child safety, hate speech and counter-terrorism, software engineers to develop review systems, quality control managers, policy specialists, legal specialists, and general reviewers.

We are also using machine learning to better detect and action on content and people that should not be using our platform. For example, we incorporated learnings from interference in previous elections to better detect and stop false accounts from spreading misinformation in more recent elections. We recently shared how we are using machine learning to prevent bad actors like terrorists or scammers from using our platform (https://www.facebook.com/notes/facebook-security/introducing-new-machine-learning-techniques-to-help-stop-scams/10155213964780766/).

For more information, see Response to Question 2.

4. Does Mr. Zuckerberg support a publicly-funded alternative to Facebook as vital American infrastructure to be regulated and maintained similar to our highway, water, sanitation, and communication systems?

Facebook faces significant competition in the many different markets in which we operate. In Silicon Valley and around the world, new social apps and apps enabling communication and sharing are emerging all the time. The average American uses eight different apps to communicate with their friends and stay in touch with people. There is a lot of choice, innovation, and activity in this space, with new competitors arising all the time.

Facebook's top priority and core service is to build useful and engaging products that enable people to connect, discover and share through mobile devices and personal computers. Given its broad product offerings, Facebook faces numerous competitors, competing to attract, engage, and retain users, to attract and retain marketers, and to attract and retain developers who build compelling mobile and web applications. For instance, if a user wants to share a photo or video, they can choose between Facebook, DailyMotion, Snapchat, YouTube, Flickr, Twitter, Vimeo, Google Photos, and Pinterest, among many other services. Similarly, if a user is looking to message someone, just to name a few, there's Apple's iMessage, Telegram, Skype, Line, Viber, WeChat, Snapchat, and LinkedIn—as well as the traditional text messaging services their mobile phone carrier provides. Equally, companies also have more options than ever when it comes to advertising—from billboards, print and broadcast, to newer platforms like Facebook, Spotify, Twitter, Google, YouTube, Amazon or Snapchat. Facebook represents a small part (in fact, just 6 percent) of this $650 billion global advertising ecosystem and much of that has been achieved by helping small businesses—many of whom could never have previously afforded newspaper or TV ads—to cost-effectively reach a wider audience.

5. Ask him why, given its technical sophistication, does it take FB so long to take down fake news and hateful postings. I've reported virulent anti-gay propaganda and saw the posts circulating on FB days later.

See Response to Question 3.

When a piece of content goes viral, we often see people change the content slightly or use slightly different language, in order to evade detection. We are working to address these gaps through a combination of technology, policy, and training improvements. We are also using machine learning to better detect and take action on content and people that violate our policies.

6. When did you first discover the improper use of user data by Cambridge or any other similarly situated company, and what steps did you take to actually enforce your agreement? What changes have you implemented concerning the manner in which Facebook supervises or otherwise audits third party use of data given this transgression?

When Facebook learned about Kogan's breach of Facebook's data use policies in December 2015, we took immediate action. The company retained an outside firm to assist in investigating Kogan's actions, to demand that Kogan and each party he had shared data with delete the data and any derivatives of the data, and to obtain certifications that they had done so. Because Kogan's app could no longer collect most categories of data due to changes in Facebook's platform, our highest priority at that time was ensuring deletion of the data that Kogan may have accessed before these changes took place. With the benefit of hindsight, we

wish we had notified people whose information may have been impacted. Facebook has since notified all people potentially impacted with a detailed notice at the top of their News Feed.

Recently, we announced a number of additional steps we're taking to address concerns raised by Kogan's app.

- **Review our platform.** We will investigate all apps that had access to large amounts of data before the platform changes we announced in 2014, and we will audit any app where we identify suspicious activity. If we identify misuses of data, we'll take immediate action, including banning the app from our platform and pursuing legal action if appropriate.

- **Tell people about data misuse.** We will tell people about apps that have misused their data.

- **Turn off access for unused apps.** If someone has not used an app within the last three months, we will turn off the app's access to their data.

- **Restrict Facebook Login data.** We are changing Login, so that the only data that an app can request without app review will include name, profile photo, and email address. Requesting any other data will require approval from Facebook. We will also no longer allow apps to ask for access to information like religious or political views, relationship status and details, custom friends lists, education and work history, fitness activity, book reading and music listening activity, news reading, video watch activity, and games activity. We will encourage people to manage the apps they use. We already show people what apps their accounts are connected to and allow them to control what data they've permitted those apps to use. But we're making it easier for people to see what apps they use and the information they have shared with those apps.

- **Reward people who find vulnerabilities.** We launched the Data Abuse Bounty program so that people can report to us any misuses of data by app developers.

- **Update our policies.** We have updated our terms and Data Policy to explain how we use data and how data is shared with app developers.

7. One thing that I'm not clear on is whether Facebook had a Facebook Employee inside Cambridge Analytica to help them with their "work." I've seen this reported both ways. If this is true, my question to Zuckerberg would be why did they feel compelled to help this company so much?

Facebook did not have an employee inside Cambridge Analytica. Facebook representatives provide general ad support to political advertisers on Facebook, as they do with other, non-political managed accounts. During the 2016 election cycle, for instance, Facebook provided identical support to both the Trump and Clinton campaigns, though no one from the company was assigned full time to either campaign.

8. CA has admitted to bribing and blackmailing to get what they need. Was he *blackmailed* or *bribed* or both into supporting this work? Did he know that CA was working solely for the Trump Campaign? What compelled him to risk everything to work for one sole campaign?

Mark Zuckerberg was not bribed or blackmailed by Cambridge Analytica. Facebook offered identical support to both the Trump and Clinton campaigns, and had teams assigned to both. Everyone had access to the same tools, which are the same tools that every campaign is offered. No one from Facebook was assigned full-time to the Trump campaign, or full-time to the Clinton campaign. Both campaigns approached things differently and used different amounts of support.

9. Why they issued a newspaper statement instead of a clear and obvious announcement via their own social media platform.

With the benefit of hindsight, we wish we had notified people whose information may have been impacted. Facebook has since notified all people potentially impacted with a detailed notice at the top of their News Feed.

10. Why is it so difficult to manage my privacy settings, who can and cannot see my personal information?

We believe that it's important to communicate with people about the information that we collect and how people can control it. That is why we work hard to provide this information to people in a variety of ways: in our Data Policy, and in Privacy Basics, which provides walkthroughs of the most common privacy questions we receive. Beyond simply disclosing our practices, we also think it's important to give people access to their own information, which we do through our Download Your Information and Access Your Information tools, Activity Log, and Ad Preferences, all of which are accessible through our Privacy Shortcuts tool. We also provide information about these topics as people are using the Facebook service itself.

We've heard loud and clear that privacy settings and other important tools are too hard to find and that we must do more to keep people informed. So, we're taking additional steps to put people more in control of their privacy. For instance, we redesigned our entire settings menu on mobile devices from top to bottom to make things easier to find. We also created a new Privacy Shortcuts in a menu where users can control their data in just a few taps, with clearer explanations of how our controls work. The experience is now clearer, more visual, and easy-to-find. Furthermore, we also updated our terms of service that include our commitments to everyone using Facebook. We explain the services we offer in language that's easier to read. We also updated our Data Policy to better spell out what data we collect and how we use it in Facebook, Instagram, Messenger, and other products.

We also recently announced plans to build Clear History. This feature will enable users to see the websites and apps that send us information when they use them, clear this information from their accounts, and turn off our ability to store it associated with their accounts going forward. Apps and websites that use features such as the Like button or Facebook Analytics send us information to make their content and ads better. We also use this information to make users'

experiences on Facebook better. If a user clears their history or uses the new setting, we'll remove identifying information so a history of the websites and apps they've used won't be associated with their account. We'll still provide apps and websites with aggregated analytics—for example, we can build reports when we're sent this information so we can tell developers if their apps are more popular with men or women in a certain age group. We can do this without storing the information in a way that's associated with a user's account, and as always, we don't tell advertisers who a user is.

11. Isn't advertising income enough? Compiling data on people and selling it is too much. Just because you're in the unique position to do it doesn't make it right. Facebook is practically a monopoly in the social media world. You're abusing your rights.

Facebook does not sell people's information to anyone, and we never will. We also impose strict restrictions on how our partners can use and disclose the data we provide.

Our Data Policy makes clear the circumstances in which we work with third-party partners who help us provide and improve our Products or who use Facebook Business Tools to grow their businesses, which makes it possible to operate our companies and provide free services to people around the world.

Further, in Silicon Valley and around the world, new social apps are emerging all the time. The average American uses eight different apps to communicate with their friends and stay in touch with people. There is a lot of choice, innovation, and activity in this space, with new competitors arising all the time.

For more information, see Response to Question 4.

12. What are the regulations on Social Media? They have a dangerous amount of personal data on us all and zero accountability. There are no alternatives to Facebook, and so people are mad but not willing to actually delete their accounts. So, I implore or elected officials to protect us when we can't seem to have the intelligence or courage to protect ourselves. It's worth mentioning that they already have the data, and leaving now doesn't undo the breach of trust.
I would also ask that we consider social media as a news source. Because it is. And yet there is no responsibility. No fiduciary role required in the best interests of the American people. Or anyone else. And we know from this experience that just because a company should do something they won't unless it A: makes them more money or B: is required by law.

Facebook is generally not opposed to regulation but wants to ensure it is the right regulation. We are already regulated in many ways—for example, under the Federal Trade Commission Act—and we are subject to ongoing oversight by the FTC under the terms of a 2011 Consent Order. Facebook has inherent incentives to protect its customers' privacy and address breaches and vulnerabilities. Indeed, the recent discovery of misconduct by an app developer on the Facebook platform clearly hurt Facebook and made it harder for us to achieve our social mission. As such, Facebook is committed to protecting our platform from bad actors, ensuring

we are able to continue our mission of giving people a voice and bringing them closer together. We are also actively building new technologies to help prevent abuse on our platform, including advanced AI tools to monitor and remove fake accounts. We have also significantly increased our investment in security, employing more than 15,000 individuals working solely on security and content review and planning to increase that number to over 20,000 by the end of the year.

13. Facebook is invasive and people early on had no idea what they were getting into. Why not force data to be erased after a period of time? For instance a 5 year sundowner policy on American citizens data with MASSIVE penalties for violation?

Our Download Your Information or "DYI" tool is Facebook's data portability tool and was launched many years ago to let people access and download many types of information that we maintain about them. The data in DYI and in our Ads Preferences tool contain each of the interest categories that are used to show people ads, along with information about the advertisers that are currently running ads based on their use of an advertiser's website or app. People also can choose not to see ads from those advertisers. We recently announced expansions to Download Your Information, which, among other things, will make it easier for people to see their data, delete it, and easily download and export it. More information is available at https://newsroom.fb.com/news/2018/04/new-privacy-protections/.

Responding to feedback that we should do more to provide information about websites and apps that send us information when people use them, we also announced plans to build Clear History. This new feature will enable users to see the websites and apps that send us information when they use them, clear this information from their account, and turn off Facebook's ability to store it associated with their account going forward.

We have also introduced Access Your Information. This feature provides a new way for people to access and manage their information. Users can go here to delete anything from their timeline or profile that they no longer want on Facebook. They can also see their ad interests, as well as information about ads they've clicked on and advertisers who have provided us with information about them that influence the ads they see. From here, they can go to their ad settings to manage how this data is used to show them ads.

14. I would like to know about any deals made between Facebook and the Obama Administration data mining Facebook users information and using it to determine which US Citizens are deemed friendly or foe and how they might vote in the 16 Election?

Facebook representatives advise political advertisers on Facebook, as they would with other, non-political managed accounts. Unlike Kogan and his company, GSR, Facebook is not aware that any Facebook app operated by the 2012 Obama for America campaign violated our Platform Policies. Further, during the 2012 election cycle, both the Obama and Romney campaigns had access to the same tools, and no campaign received any special treatment from Facebook.

15. Facebooks forces the user to 'trust' them with their data when they sign up, or they cannot create an account. The same applies to most platforms as well as in other

areas, like credit reporting. Why shouldn't there be criminal penalties for misusing, or losing, our data?

Sharing posts and information about yourself is a core part of using Facebook, and people agree to our Data Policy—which describes how we collect, use, and share data—as a part of using Facebook.

Protecting people's information is essential to Facebook's success, since we know people won't feel comfortable using Facebook if they don't have confidence their information is protected. That's why we work hard to build privacy improvements into Facebook, including the changes we made limiting developer access to friends data in 2014, and the improvements we're making now to be sure this doesn't happen again.

We've heard loud and clear that privacy settings and other important tools are too hard to find and that we must do more to keep people informed. So, we're taking additional steps to put people more in control of their privacy. For instance, we redesigned our entire settings menu on mobile devices from top to bottom to make them easier to find and use. We also created a new Privacy Shortcuts in a menu where users can control their data in just a few taps, with clearer explanations of how our controls work. The experience is now clearer, more visual, and easy-to-find. Furthermore, we also updated our terms of service that include our commitments to everyone using Facebook. We explain the services we offer in language that's easier to read. We've also updated our Data Policy to better spell out what data we collect and how we use it in Facebook, Instagram, Messenger, and other products we provide.

Further, Facebook is regulated in the US by the FTC, which exercises oversight over the privacy practices covered under our consent decree.

16. Why do they allow dark ads that are only seen by the recipient?

We have launched "View Active Ads" globally, a feature that will enable anyone to see all of the ads an advertiser is currently running by visiting the advertiser's Facebook Page. This level of transparency is unprecedented among advertising platforms, and it will give people the opportunity to see ads regardless of whether they are in the target audience.

17. Will they notify directly the FB users who saw the Russian FB ads?

We launched a portal to enable people on Facebook to learn which of the IRA Facebook Pages or Instagram accounts they may have liked or followed between January 2015 and August 2017. This tool is available in the Facebook Help Center. We took steps to make users aware of this tool, including through a notification in the News Feed of users who were most likely to be affected. The ads run by the IRA are also available at https://democrats-intelligence.house.gov/facebook-ads/.

The Honorable Michael Doyle

1. Please provide unredacted copies of any audits Facebook was required to perform as part of Facebook's 2011 Consent Decree Agreement with Federal Trade Commission.

The privacy assessments conducted by PwC contain both Facebook's and PwC's sensitive business information that are confidential in order to prevent competitive harm and to ensure the integrity of Facebook's privacy program, including the steps that we take to protect people's information. We have furnished these reports to the FTC and are prepared to review the reports with regulators and lawmakers with appropriate assurances that confidential information or information that could be exploited to cause competitive harm or to circumvent Facebook's privacy protections will not be disclosed publicly.

2. Please provide an unredacted copy of the Pricewaterhouse Coopers report entitled "Independent Assessor's report on Facebook's Privacy Program" for the period of February 12, 2015 to February 11, 2017.

See Response to Question 1.

3. Please provide a list of developers that Facebook has taken legal action against for violations of Facebook's developer policy. Included in that list, please indicate the developer violation, the specific action or actions Facebook took against the party, and the dates of the violation and the actions.

We use a variety of tools to enforce Facebook policies against violating parties, including developers. We review tens of thousands of apps per year and regularly disapprove noncompliant apps as part of our proactive review process. We also use tools like cease-and-desist letters, account suspensions, letter agreements, and civil litigation. For example, since 2006, Facebook has sent over 1,150 cease-and-desist letters to over 1,600 targets. In 2017, we took action against about 370,000 apps, ranging from imposing certain restrictions to removal of the app from the platform. Moreover, we have required parties who have procured our data without authorization to delete that data. We have invested significant resources in these efforts. Facebook is presently investigating apps that had access to large amounts of information before we changed our platform policies in 2014 to significantly reduce the data apps could access. As of early June 2018, around 200 apps (from a handful of developers: Kogan, AIQ, Cube You, the Cambridge Psychometrics Center, myPersonality, and AIQ) have been suspended—pending a thorough investigation into whether they did in fact misuse any data.

Additionally, we have suspended an additional 14 apps, which were installed by around one thousand people. They were all created after 2014, after we made changes to more tightly restrict our platform APIs to prevent abuse. However, these apps appear to be linked to AIQ, which was affiliated with Cambridge Analytica. So, we have suspended them while we investigate further. Any app that refuses to take part in or fails our audit will be banned.

4. Did Facebook specifically take legal action against any developer for violations of the Facebook's developer policy for the unauthorized sharing of Facebook data with

a third party? If so please describe the violation, describe the action Facebook took to address the violation, and the dates of these events.

See Response to Question 3.

5. In your testimony before the Committee, you mentioned that Aleksandr Kogan sold Facebook user data to parties besides Cambridge Analytica. Please provide a list of any other entity that Kogan sold or provided this data to.

Kogan represented that, in addition to providing data to his Prosociality and Well-Being Laboratory at the University of Cambridge for the purposes of research, GSR provided some Facebook data to SCL Elections Ltd., Eunoia Technologies, and the Toronto Laboratory for Social Neuroscience at the University of Toronto. However, the only party Kogan has claimed paid GSR was SCL. Our investigation is ongoing.

6. Does Facebook have any commercial relationships or any research partnerships with Palantir? If so please describe the type and nature of each.

Palantir was founded by Facebook Board Member Peter Thiel. Thiel has served on Facebook's Board since April 2005.

The Honorable Jan Schakowsky

1. In a post dated March 21, 2018, on your Facebook page, you announced that Facebook is investigating all apps that had access to large amounts of information before Facebook changed its platform in 2014. At the hearing on April 11, 2018, I asked you how long it was going to take Facebook to complete its investigations of all of the apps on Facebook. There have been many conflicting reports of how many apps are actually on Facebook and were on Facebook at the time of the Cambridge Analytica incident. I want to get a better grasp on the scope of the investigations.

a. How many apps were using the Facebook platform when Aleksandr Kogan created the personality quiz app in 2013?

Facebook is in the process of investigating all the apps that had access to large amounts of information, such as extensive friends data (if those friends' privacy data settings allowed sharing), before we changed our platform policies in 2014—significantly reducing the data apps could access. Where we have concerns about individual apps, we are investigating them—and any app that either refuses or fails an audit will be banned from Facebook. As of early June 2018, thousands of apps have been investigated and around 200 have been suspended—pending a thorough investigation into whether they did in fact misuse any data.

These apps relate to a handful of developers: Kogan, AIQ, Cube You, the Cambridge Psychometrics Center, and myPersonality, with many of the suspended apps being affiliated with the same entity. Many of these apps also appear to be "test" apps that were never released to the public, and therefore would not have acquired significant user data, although our investigation into these apps is ongoing.

Additionally, we have suspended an additional 14 apps, which were installed by around one thousand people. They were all created after 2014, after we changed our platform to reduce data access. However, these apps appear to be linked to AIQ, which was affiliated with Cambridge Analytica. So, we have suspended them while we investigate further. Any app that refuses to take part in or fails our audit will be banned.

b. How many apps were using the Facebook platform when Facebook changed the platform to disallow friends-of-friends data from being accessed in 2014?

See Response to Question 1(a).

c. How many apps were using the Facebook platform when *The Guardian* first reported that Kogan shared data from his app with Cambridge Analytica in 2015?

In the ninety days leading up to *The Guardian* article, published December 12, 2015, there were approximately 2 million active apps active on Facebook.

d. We were told that when Facebook announced changes to the platform policy in 2014 that limited the data apps could access, Facebook gave app

developers some time to come into compliance. Please provide the date that the policy changes were announced and the date by which apps were required to be in compliance.

In April 2014, we announced that we would more tightly restrict our platform APIs to prevent abuse. At that time, we made clear that existing apps would have a year to transition—at which point they would be forced (1) to migrate to the more restricted API and (2) be subject to Facebook's new review and approval protocols. The vast majority of companies were required to make the changes by May 2015; a small number of companies (fewer than 100) were given a one-time extension of less than six months beyond May 2015 to come into compliance. (One company received an extension to January 2016.) In addition, in the context of our ongoing review of third-party apps, we discovered a very small number of companies (fewer than 10) that theoretically could have accessed limited friends' data as a result of API access that they received in the context of a beta test. We are not aware that any of this handful of companies used this access, and we have now revoked any technical capability they may have had to access any friends' data. New apps that launched after April 30, 2014 were required to use our more restrictive platform APIs.

e. After the date that all apps were to be in compliance with the new policy, were exceptions given to any apps to permit those apps access to data of friends of the app user? Please list all apps that were given such exemptions and list when such exemptions were terminated or expired.

See Response to Question 1(d).

f. How many apps are currently using the Facebook platform?

As of about the end of April 2018, there had been approximately 1.8 million apps and roughly 1.5 million developers active on Facebook over the prior two months.

g. In your March 21 post, you said that Facebook is investigating "all apps that had access to large amounts of information" before the change in the platform in 2014. What do you mean by "large amounts of information"? How many apps are you actually investigating?

Our investigation is ongoing and as part of it we are taking a close look at applications that had access to friends data under Graph API V1 before we made technical changes to our platform to change this access.

See Response to Question 1(a).

h. What do you expect to learn from the investigations? What will investigations entail other than audits? Please explain how audits will be conducted?

See Response to Question 1(a).

We will investigate all apps that had access to large amounts of data before the platform changes we announced in 2014, and among other things, analyze potentially suspicious activity from our analysis of logs and usage patterns by these apps. Where we have concerns, we will conduct an audit using internal and external experts and ban any developer that refuses to comply. If we identify misuses of data, our enforcement actions may include banning the app from our platform and pursuing legal action if appropriate.

i. How will you be able to determine whether app developers shared or sold data obtained from Facebook with outside parties? Will you audit or otherwise investigate any outside parties that Facebook learns had access to Facebook users data?

See Response to Question 1(a).

j. How will you audit app developers that are no longer in business? Will you be able to audit all apps that have the data they collected stored in other countries? How will Facebook audit or otherwise investigate those apps for which you may not be able to get access to their servers?

See Response to Question 1(a).

k. Please share the timeline or benchmarks, if any, Facebook has established to complete this investigation.

See Response to Question 1(a).

2. You promised that Facebook will ban apps that misused data and notify affected users. What about the data itself? Facebook asked Cambridge Analytica to delete the improperly acquired user data. But Cambridge Analytica reportedly also made a derivative psychographic data set using Facebook users' data.

a. Has Facebook requested that Cambridge Analytica delete the derivative sets of data that were created using obtained Facebook users' data? Has Cambridge Analytica deleted such derivative data sets? Please describe in detail how Facebook has verified that Cambridge Analytica has deleted such derivative data sets.

On December 11, 2015, *The Guardian* published an article reporting that Kogan and his company, GSR, may have passed information the app had obtained from Facebook users to SCL Elections Ltd. (SCL)/Cambridge Analytica. Kogan and his company violated Facebook's Platform Policies, which explicitly prohibited selling user data accessed from Facebook and from sharing any user data accessed from Facebook with any ad network, data broker or other advertising or monetization related service.

For this reason, Facebook immediately banned the app from our platform and investigated what happened and what further action we should take to enforce our Platform Policies. Facebook also contacted Kogan/GSR and demanded that they explain what data they collected, how they used it, and to whom they disclosed it. Facebook further insisted that Kogan

and GSR, as well as other persons or entities to whom they had disclosed any such data, account for and irretrievably delete all such data and information.

Facebook also contacted Cambridge Analytica to investigate the allegations reflected in the reporting. On January 18, 2016, Cambridge Analytica provided written confirmation to Facebook that it had deleted the data received from Kogan and that its server did not have any backups of that data. On June 11, 2016, Kogan executed signed certifications of deletion on behalf of himself and GSR. The certifications also purported to identify all of the individuals and entities that had received data from GSR (in addition to Kogan and his lab), listing the following: SCL, Eunoia Technologies (a company founded by Christopher Wylie), and a researcher at the Toronto Laboratory for Social Neuroscience at the University of Toronto. On July 7, 2016, a representative of the University of Toronto certified that it deleted any user data or user-derived data. On August 16, 2016, Eunoia (executed by Eunoia Founder Christopher Wylie) certified that it deleted any user and user-derived data. On September 6, 2016, counsel for SCL informed counsel for Facebook that SCL had permanently deleted all Facebook data and derivative data received from GSR and that this data had not been transferred or sold to any other entity. On April 3, 2017, Alexander Nix, on behalf of SCL, certified to Facebook, that it deleted the information that it received from GSR or Kogan.

Because all of these concerns relate to activity that took place off of Facebook and its systems, we have no way to confirm whether Cambridge Analytica may have Facebook data without conducting a forensic audit of its systems. Cambridge Analytica has agreed to submit to a forensic audit, but we have not commenced that yet due to a request from the UK Information Commissioner's Office, which is simultaneously investigating Cambridge Analytica (which is based in the UK). And even with an audit, it may not be possible to determine conclusively what data was shared with Cambridge Analytica or whether it retained data after the date it certified that data had been deleted.

The existing evidence that we are able to access supports the conclusion that Kogan only provided SCL with data on Facebook users from the United States. While the accounts of Kogan and SCL conflict in some minor respects not relevant to this question, both have consistently maintained that Kogan never provided SCL with any data for Facebook users outside the United States. These consistent statements are supported by a publicly released contract between Kogan's company and SCL.

In March 2018, we learned from news reports that contrary to the certifications given, not all of the Kogan data may have been deleted by Cambridge Analytica. We have no direct evidence of this and no way to confirm this directly without accessing Cambridge Analytica's systems and conducting a forensic audit. We have held off on audits of Cambridge Analytica and other parties that are being investigated by the UK Information Commissioner's Office at its request. Our investigation is ongoing.

b. How is Facebook investigating other firms that may have obtained Facebook users' data or derivative data sets from Cambridge Analytica? If Facebook discovers entities that have obtained from or otherwise rely on Facebook users' data or derivative data sets ever held by Cambridge Analytica, what actions will Facebook take with respect to those firms?

See Response to Question 2(a).

c. In your investigations of apps that had access to large amounts of information before Facebook changed its platform in 2014, are you also investigating whether apps or other companies used that information to make derivative data sets like the psychographic information created by Cambridge Analytica? Have you identified any other firms that have created derivative data sets to date?

We are in the process of investigating every app that had access to a large amount of information before we changed our Platform in 2014. The investigation process is in full swing, and it has two phases. First, a comprehensive review to identify every app that had access to this amount of Facebook data and to focus on apps that present reason for deeper investigation. And second, where we have concerns, we will conduct interviews, make requests for information (RFI)—which ask a series of detailed questions about the app and the data it has access to—and perform audits using expert firms that may include on-site inspections. We have large teams of internal and external experts working hard to investigate these apps as quickly as possible. As of early June 2018, thousands of apps have been investigated and around 200 apps have been suspended—pending a thorough investigation into whether they did in fact misuse any data. Where we find evidence that these or other apps did misuse data, we will ban them and let people know.

These apps relate to a handful of developers: Kogan, AIQ, Cube You, the Cambridge Psychometrics Center, and myPersonality, with many of the suspended apps being affiliated with the same entity. Many of these suspensions include apps that appear to be "test" apps that were never released to the public, and therefore would not have acquired significant user data, although our investigation into these apps is ongoing.

Additionally, we have suspended an additional 14 apps, which were installed by around one thousand people. They were all created after 2014, after we made changes to more tightly restrict our platform APIs to prevent abuse. However, these apps appear to be linked to AIQ, which was affiliated with Cambridge Analytica. So, we have suspended them while we investigate further. Any app that refuses to take part in or fails our audit will be banned.

We will commit to briefing your staff on future developments.

d. Has Facebook requested or will Facebook request that any other firms delete derivative data sets? Have any firms done so? Please describe in detail how Facebook has verified that these other firms have deleted such derivative data sets.

See Response to Question 2(c).

3. At the hearing, I asked how many other firms Mr. Kogan sold data to and what the names of those firms are. You said you would have to get back to me.

a. Please list the names of all firms to whom Mr. Kogan sold Facebook users' data, and if there are any that you have not yet identified, please provide the total number of firms to whom Mr. Kogan sold Facebook users' data.

b. Did Facebook know in 2015 that Mr. Kogan sold Facebook users' data to firms other than Cambridge Analytica? Please list those firms. Did Facebook request that those firms delete all Facebook users' data that they had acquired from Mr. Kogan at that time? Did Facebook request that those films delete all derivative data sets that were created using obtained Facebook users' data at that time? How did Facebook confirm that these data sets were deleted at that time?

See Response to Question 2(a).

4. At the Senate hearing on April 10, 2018, you said, "You are not allowed to have a fake account on Facebook." Yet last November Facebook itself estimated up to 270 million accounts are fake or duplicate.

a. How many accounts does Facebook currently estimate are fake or duplicate? How often will Facebook commit to reporting those estimates going forward?

We estimate that fake accounts represented approximately 3% to 4% of monthly active users (MAU) on Facebook during Q1 2018 and Q4 2017. We share this number in the Facebook quarterly financial results. This estimate may vary each quarter based on spikes or dips in automated fake account creation.

b. Your testimony only said that Facebook will be requiring people who manage large pages to be verified. What exactly do you mean by "large pages"?

We have announced that people who manage Pages with large numbers of followers will need to be verified. Those who manage large Pages that do not clear the process will no longer be able to post. This will make it much harder for people to administer a Page using a fake account, which is strictly against our policies. We will also show users additional context about Pages to effectively assess their content. For example, a user can see whether a Page has changed its name.

c. We now know that fake accounts were part of Russia's manipulation of the 2016 election. Would any of the pages used by Russian operatives not be classified as large pages"?

We are committed to finding and removing fake accounts. We continue to make improvements to our efforts to more effectively detect and deactivate fake accounts to help reduce the spread of spam, false news, and misinformation. We continually update our technical systems to identify, checkpoint, and remove inauthentic accounts, and we block millions of attempts to register fake accounts every day. These systems examine thousands of detailed account attributes and prioritize signals that are more difficult for bad actors to disguise, such as their connections to others on our platform. As with all security threats, we have been

incorporating new insights into our models for detecting fake accounts, including information specific to election issues.

We do not share detailed descriptions of how our tools work in order to avoid providing a road map to bad actors who are trying to avoid detection. When we suspect that an account is inauthentic, we typically enroll the account in a checkpoint that requires the account holder to provide additional information or verification. We view disabling an account as a severe sanction, and we want to ensure that we are highly confident that the account violates our policies before we take permanent action. When we have confirmed that an account violates our policies, we remove the account.

d. What actions is Facebook taking to track and delete activity by fake accounts beyond large pages?

See Response to Question 4(c).

e. It seems that every few weeks we see a tiny amount of progress being reported, but then the social media bots spring back to life unabated. What specifically is Facebook doing to shut down these bots?

Stopping the abuse of fake accounts and malicious bot activity is a focus for many teams, some more directly and some in more of a supportive role. For example, we are expanding our threat intelligence team, and more broadly, we are working now to ensure that we will more than double the number of people working on safety and security at Facebook, from 10,000 to 20,000, by the end of 2018. We expect to have at least 250 people specifically dedicated to safeguarding election integrity on our platforms, and that number does not include the thousands of people who will contribute to this effort in some capacity. Many of the people we are adding to these efforts will join our ad review team, and we also expect to add at least 3,000 people to Community Operations, which reviews content that our users and automated tools flag as inappropriate, dangerous, abusive, or otherwise violating our policies. We also continue to make improvements to our efforts to more effectively detect and deactivate fake accounts to help reduce the spread of spam, false news, and misinformation. We continually update our technical systems to identify, checkpoint, and remove inauthentic accounts, and we block millions of attempts to register fake accounts every day. These systems examine thousands of detailed account attributes and prioritize signals that are more difficult for bad actors to disguise, such as their connections to others on our platform. As with all security threats, we have been incorporating new insights into our models for detecting fake accounts, including information specific to election issues.

We publish information and metrics about fake accounts at https://transparency.facebook.com/community-standards-enforcement#fake-accounts and in our quarterly SEC filings.

5. I'd like to touch on an issue of great concern to the more than one thousand Rohingyas who have relocated to the Chicago area since 2010. You said Facebook will improve the mechanism to report content in Facebook Messenger and add Burmese-speaking reviewers. Here's the challenge I see: you generally want users

to be free to post content without censorship, but you also do not want Facebook to be a platform for encouraging genocide. Facebook is in the position of deciding what is legitimate speech and what may potentially incite violence.

a. How much does Facebook's approach to harmful content still rely on third parties to flag violence-inciting content?

b. How do you make those decisions? Does Facebook have the capacity to be a fair arbiter?

We've been too slow in Myanmar to deal with the hate and violence. We are investing in people, technology and programs to help address these very serious challenges.

We are working to strike the right balance between enabling free expression around the globe and ensuring that our platform is safe. Our Community Standards prohibit hate speech and celebrating graphic violence, and allow people to use Facebook to raise awareness of and condemn violence. Drawing that line requires complex and nuanced judgments, and we carefully review reports that we receive from the public, media, civil society, and governments. We remove content that violates our policies, regardless of who posted the content (including the government). We have teams who are fluent in the local language not only to review content, but also to work with local organizations to help us understand and address the deep challenges stemming from these types of conflicts. In addition to responding to reports, we have been working with local communities and NGOs for years in these regions to educate people about hate speech, news literacy, and our polices. For example, we have introduced an illustrated, Myanmar language-specific copy of our community standards and a customized safety Page, which we work with our local partners to promote, and we recently ran a series of public service ads in Myanmar that we developed with the News Literacy Project to help inform people about these important issues.

We encourage people to report posts and rely on our team of content reviewers around the world to review reported content. Our reviewers are trained to look for violations and enforce our policies consistently and as objectively as possible. We have weekly quality audits of each reviewer, during which we re-review a subset of their work and address any mistakes made. We receive millions of reports of possible content violations every week, so we know that we will unfortunately make many mistakes even if we maintain an accuracy rate of 99 percent. We are always working to make our platform safer and more secure through, among other things, continually evaluating our processes, policies, and training. Enforcement is never perfect, but we will get better at finding and removing improper content.

6. Earlier this year, Special Counsel Robert Mueller filed an indictment against the Internet Research Agency (IRA), a Russian organization, alleging its creation of fake social- media accounts to sow discord and interfere with elections.

a. Recently, you talked about new tools that Facebook has been rolling out since the 2016 election to combat the IRA and other so-called troll farms. How do you know that these new tools are effective? What criteria are you using to measure effectiveness?

b. How confident are you that Facebook can detect and quickly identify all the fake and automated accounts?

c. Can you commit that the 2018 midterm elections in the U.S. won't be subject to the IRA or other troll farms?

d. Can you commit that the ways the Russians or others used Facebook to influence the 2016 U.S. elections and the UK's Brexit election will not happen again?

In the run-up to the 2016 elections, we were focused on the kinds of cybersecurity attacks typically used by nation states, for example phishing and malware attacks. And we were too slow to spot this type of information operations interference. Since then, we've made important changes to prevent bad actors from using misinformation to undermine the democratic process.

This will never be a solved problem because we're up against determined, creative and well-funded adversaries. But we are making steady progress. Here is a list of the 10 most important changes we have made:

- **Ads transparency.** Advertising should be transparent: users should be able to see all the ads an advertiser is currently running on Facebook, Instagram and Messenger. And for ads with political content, we've created an archive that will hold ads with political content for seven years—including information about ad impressions and spend, as well as demographic data such as age, gender and location. People in Canada and Ireland have already been able to see all the ads that a Page is running on Facebook—and we've launched this globally.

- **Verification and labeling.** Every advertiser will now need to confirm their ID and location before being able to run any ads with political content in the US. All ads with political content will also clearly state who paid for them.

- **Updating targeting.** We want ads on Facebook to be safe and civil. We thoroughly review the targeting criteria advertisers can use to ensure they are consistent with our principles. As a result, we removed nearly one-third of the targeting segments used by the IRA. We continue to allow some criteria that people may find controversial. But we do see businesses marketing things like historical books, documentaries or television shows using them in legitimate ways.

- **Better technology.** Over the past year, we've gotten increasingly better at finding and disabling fake accounts. We now block millions of fake accounts each day as people try to create them—and before they've done any harm. This is thanks to improvements in machine learning and artificial intelligence, which can proactively identify suspicious behavior at a scale that was not possible before—without needing to look at the content itself.

- **Action to tackle fake news.** We are working hard to stop the spread of false news. We work with third-party fact-checking organizations to limit the spread of articles

rated false. To reduce the spread of false news, we remove fake accounts and disrupt economic incentives for traffickers of misinformation. We also use various signals, including feedback from our community, to identify potential false news. In countries where we have partnerships with independent third-party fact-checkers, stories rated as false by those fact-checkers are shown lower in News Feed. If Pages or domains repeatedly create or share misinformation, we significantly reduce their distribution and remove their advertising rights. We also want to empower people to decide for themselves what to read, trust, and share. We promote news literacy and work to inform people with more context. For example, if third-party fact-checkers write articles about a news story, we show them immediately below the story in the Related Articles unit. We also notify people and Page Admins if they try to share a story, or have shared one in the past, that's been determined to be false. In addition to our own efforts, we're learning from academics, scaling our partnerships with third-party fact-checkers and talking to other organizations about how we can work together.

A key focus is working to disrupt the economics of fake news. For example, preventing the creation of fake accounts that spread it, banning sites that engage in this behavior from using our ad products, and demoting articles found to be false by fact checkers in News Feed—causing it to lose 80% of its traffic. We now work with independent fact checkers in the US, France, Germany, Ireland, the Netherlands, Italy, Mexico, Colombia, India, Indonesia and the Philippines with plans to scale to more countries in the coming months.

- **Significant investments in security.** We're doubling the number of people working on safety and security from 10,000 last year to over 20,000 this year. We expect these investments to impact our profitability. But the safety of people using Facebook needs to come before profit.

- **Industry collaboration.** Recently, we joined 34 global tech and security companies in signing a TechAccord pact to help improve security for everyone.

- **Information sharing and reporting channels.** In the 2017 German elections, we worked closely with the authorities there, including the Federal Office for Information Security (BSI). This gave them a dedicated reporting channel for security issues related to the federal elections.

- **Tracking 40+ elections.** In recent months, we've started to deploy new tools and teams to proactively identify threats in the run-up to specific elections. We first tested this effort during the Alabama Senate election, and plan to continue these efforts for elections around the globe, including the US midterms. Last year we used public service announcements to help inform people about fake news in 21 separate countries, including in advance of French, Kenyan and German elections.

- **Action against the Russia-based IRA.** In April, we removed 70 Facebook and 65 Instagram accounts—as well as 138 Facebook Pages—controlled by the IRA primarily targeted either at people living in Russia or Russian-speakers around the world including from neighboring countries like Azerbaijan, Uzbekistan and Ukraine.

The IRA has repeatedly used complex networks of inauthentic accounts to deceive and manipulate people in the US, Europe and Russia—and we don't want them on Facebook anywhere in the world.

7. At the hearing, Congressman Butterfield asked you about minority representation at Facebook and in the tech industry generally. I'm concerned that the lack of people of color at Facebook may be leading to bias in your algorithms. Earlier this Congress our Committee held a hearing on the prevalence of bias on social media platforms and algorithms. Last year, *Pro Publico*, did a story called "Facebook's Secret Censorship Rules Protect White Men from Hate Speech But Not Black Children." Systemic bias on social media platforms is a huge problem for communities of color. Obviously, Facebook cannot address all instances of bias. But Facebook can make sure that the platform itself does not operate in a biased way.

a. Please describe in detail the steps is Facebook taking to address bias in its algorithms?

b. Will you commit to bringing in outside, third-party experts to audit Facebook's processes and report back to us on how effective your strategy is for addressing bias caused by your platform specifically within six months?

Relman, Dane & Colfax, a respected civil rights law firm, will carry out a comprehensive civil rights assessment of Facebook's impact on underrepresented communities and communities of color. Laura Murphy, a national civil liberties and civil rights leader, will help guide this process and is getting feedback directly from civil rights groups to help advise Facebook on the best path forward.

Regarding Facebook's algorithm, a person's News Feed is made up of stories from their friends, Pages they've chosen to follow and groups they've joined. Ranking is the process we use to organize all of those stories so that people can see the most relevant content at the top, every time they open Facebook. Ranking has four elements: the available inventory of stories; the signals, or data points that can inform ranking decisions; the predictions we make, including how likely we think a person is to comment on a story, share with a friend, etc.; and a relevancy score for each story.

News Feed considers thousands of signals to surface the content that's most relevant to each person who uses Facebook. Our employees don't determine the ranking of any specific piece of content. To help the community understand how News Feed works and how changes to News Feed affect their experience on Facebook, we publish a regularly-updated Inside Feed blog (https://newsroom.fb.com/news/category/inside-feed/) where our team shares details of significant changes.

8. Facebook recently announced that it is shutting down the Partner Categories program to "help improve people's privacy on Facebook." The program gave advertisers the benefit of data from seven third-party data broker partnered with

Facebook to add to Facebook's own data about users to better target ads at those users.

a. Through that program, Facebook purchased data from the third-party data brokers to help advertisers target ads. The third-party data brokers would receive a portion of the proceeds from the sale of the ad. Is that correct?

Data partners received payments from Facebook for the use of Partner Categories, primarily based on their usage by advertisers.

b. So by shutting down this program, Facebook is actually keeping more money from the ad sale, right?

No. The total cost of the media will now reflect that there is no percentage paid for Partner Categories. In many cases, average cost should generally go down for advertisers.

c. Did anyone—the third-party data brokers, the advertiser, or anyone else—get access to any Facebook users' data through this program?

Third parties did not get access to Facebook user data through this program.

d. If no one outside of Facebook was able to access Facebook users' data, how does shutting down this program "help improve people's privacy on Facebook"?

While advertisers working with data providers is common industry practice, we think there is more we can do to improve people's experiences when it comes to third-party data use. As a first step, we decided to wind down Partner Categories. We're always working to build more transparency and accountability into advertising on Facebook.

9. More than 98 percent of Facebook's revenue is generated from advertising. You have touted that companies advertise on Facebook because all of the data you collect on individuals allows for the delivery of highly targeted messages. In fact, just last year reporters were able to buy advertising targeting anti-Semitic groups and individuals. At the time, you said that these categories were created by algorithms, not individuals, and have since been removed.

a. How does Facebook oversee the advertising categories created by algorithms? How many employees monitor those categories?

b. How many advertising categories are there total?

c. How can you assure us that similar offensive categories for targeted advertising have been removed?

In September 2017, we temporarily disabled some of our ad tools following news reports that slurs or other offensive language could be used as targeting criteria for advertising. In order to allow businesses—especially small ones—to find customers who might be interested in their

specific products or services, we offered them the ability to target profile field categories like education and employer. So, if someone on Facebook self-identified as a "Jew-hater" or said that they studied "how to burn Jews" in their education or employer fields on their profile, those terms showed up as potential targeting options for advertisers. These deeply offensive terms were used so infrequently in these write-in fields that we did not discover this until a journalist brought it to our attention.

We have long prohibited hate on Facebook, and although we are not aware of instances in which these terms were ever used to actually target ads, we take our failure to enforce that policy with caution and care in this instance extremely seriously. We never intended or anticipated that this functionality would be used this way, and we did not find it ourselves. We are accountable for these failures. We have tried to learn everything that we can from this painful incident so that we can do better in the future. We have tightened our ad policies and have taken steps to improve our enforcement, including by adding more oversight of our automated review processes, and have been exploring how best to implement tools for people to tell us when our systems may inadvertently enable abuse. We have also used human reviewers to manually check existing targeting options and reinstate the roughly 15,000 most commonly used targeting terms—terms like "nurse" or "dentistry"—to ensure that they are consistent with our advertising principles. We will do more manual review of new targeting options going forward to help prevent offensive terms from appearing. Targeted advertising on Facebook has helped millions of businesses grow, find customers, and hire people. Our systems match organizations with potential customers who may be interested in their products or services. The systems have been particularly powerful for small businesses, who can use tools that previously were only available to advertisers with large budgets or sophisticated marketing teams. Our ads help make meaningful connections between business and people, and the improvements we are making to our ad policies will help us do this more effectively.

10. Facebook recently announced that it will increase advertising transparency by requiring all advertisers to have a Facebook page where all of their ads will be posted. I understand this is being piloted in Canada.

a. When will this program be introduced in the US?

b. Will the advertisement indicate each user category it was intended to target?

c. The FTC polices deceptive advertisements where it's unclear whether a post is a paid promotion. Will Facebook make it a priority to help stop this type of deceptive advertising on its platform?

We believe that when people visit a Page or see an ad on Facebook it should be clear who it's coming from. We also think it's important for people to be able to see the other ads a Page is running, even if they're not directed at them. We want to set a new standard for advertising transparency online.

- In Canada and Ireland, we've been testing a new feature called View Ads that lets people see the ads a Page is running—even if they are not in their News Feeds. This applies to all advertiser Pages on Facebook—not just Pages running political ads.

- We just launched View Active Ads globally.

- We have also launched an archive of ads identified to contain political content (self-reported or that we have been able to identify), available at https://www.facebook.com/politicalcontentads.

- The archive will hold ads identified to contain political content for seven years so they can be searched by keyword or the Page that ran them. It also will display general information about the amount spent on the ad, the number of people who saw it, plus aggregated, anonymized data on their age, gender and location

All paid advertisements on Facebook bear a label that reads "Sponsored," which clearly distinguishes them from organic content on Facebook. In addition, our Pages terms (https://www.facebook.com/policies/brandedcontent/) and Ads Policy (https://www.facebook.com/policies/ads/#restricted_content) allow certain types of branded content on Facebook and require publishers and influencers to tag the marketer in the post to make it clear that the post is branded content. For example, a juice brand may work with a parenting blogger to have their brand or product mentioned in a post on Facebook, or a car manufacturer and a sports network may create a collaborative post aimed at sports fans about the car. Publishers and influencers remain responsible for complying with applicable law, including Section 5 of the FTC Act.

11. Despicable content spreading on the internet is not a new problem. The National Center for Missing and Exploited Children has been working to stop the spread of child pornography on the internet for years. With its partners, it developed a system called Photo DNA to block users from posting known child pornography pictures. I understand that Facebook has taken some similar steps to curb violent extremists, and I have questions about those efforts.

a. Photo DNA works so well because its database of known pornography is shared across the internet with other platforms. Can you commit to working with other platforms to share data about known problematic content used by terrorist organizations?

b. When can we expect new meaningful action on this front?

At last year's EU Internet Forum, Facebook, Microsoft, Twitter, and YouTube declared our joint determination to curb the spread of terrorist content online. Over the past year, we have formalized this partnership with the launch of the Global Internet Forum to Counter Terrorism (GIFCT). The GIFCT is committed to working on technological solutions to help thwart terrorists' use of our services, including through a shared industry hash database, where companies can create "digital fingerprints" for terrorist content and share it with participating companies. The database, which became operational in the spring of 2017, now includes 13 companies that contribute to it and contains more than 88,000 hashes. It allows the thirteen member companies to use those hashes to identify and remove matching content—videos and images—that violate our respective policies or, in some cases, block terrorist content before it is even posted. GIFCT also created an online resource for smaller tech companies to seek support

and feedback. Each company has different policies, practices, and definitions as they relate to terrorist content. If content is removed from a company's platform for violating that platform's individual terrorism-related content policies, the company may choose to hash the content and include it in the database.

12. An appalling number of teens report being bullied. Physical playground bullying is bad enough, but increasingly this cruelty is moving online, where one click of a button sends hateful words that can be seen by hundreds or thousands of people. Worse yet, these actions cannot be erased and may follow their victims forever.

According to studies published in the last year, Facebook and Instagram are the social media tools of choice for cyberbullying. Cyberbullying can take different forms, including hurtful words about a user's appearance in a photo, private information or photos published without permission, or belittling posts or private messages.

a. How many reports of cyberbullying does Facebook receive each month? How about Instagram?

b. Other than investigating these reports, what actions are taken in response to these reports?

c. What measures do Facebook and Instagram take to prevent cyberbullying from occurring?

Bullying online is a serious problem that almost always is connected to offline bullying and we have taken numerous steps not only to prevent bullying on our platform but to address the nexus between offline and online bullying.

Our policies prohibit bullying on Facebook. We want people to feel safe when using Facebook, and will remove reported content that appears to purposefully target private individuals with the intention of degrading or shaming them. The content we remove includes, but is not limited to:

- posts that identify and shame private individuals,
- images altered to degrade private individuals,
- photos or videos of physical bullying posted to shame the victim, and
- repeatedly targeting other people with unwanted friend requests or messages.

Our content reviewers respond to millions of reports each week from people all over the world. We encourage our users to report content that may violate our policies. Our Community Operations team—which is growing significantly over the next year—works around the world, 24 hours a day, and in over 50 languages to review these reports. Our automated systems also assist in the fight against bullying and harassment. For example, we use automated tools to help identify potential hate speech and other abusive content. Facebook encourages users to report to

us bullying and harassment, as well as other content that may violate our policies. Our Community Operations team works hard to review those reports and takes action when content violates our policies.

In addition to reporting, we offer social resolution tools developed with the University of California, Berkeley and the Yale Center for Emotional Intelligence. These tools give people the opportunity to use our report links to send a message to the person who posted the content that upsets them asking them to take it down and provide language prompts to help facilitate that interaction. In most cases, people will take things off Facebook if a friend asks them to.

We also offer people a number of tools to control what they see and with whom they interact to help manage their experience on our platform. People can:

- Block someone, which prevents the other person from seeing things the user posts on his/her profile; starting conversations with the user; adding the user as a friend; tagging the user in posts, comments, or photos; and inviting the user to events or groups.

- Unfriend someone, which prevents the other person from posting on the user's timeline.

- Block someone's messages, which means they will no longer be able to contact the user in Messenger or in Facebook chat. A user can also ignore a Messenger conversation, which automatically moves it out of the user's inbox.

- Unfollow someone, which means the person's post will not appear in News Feed.

- People can also use our snooze feature to temporarily block someone's posts from appearing in their New Feed.

- On Instagram, a user can prevent someone from commenting on the user's photos and videos and can also block someone from finding the user's profile, posts or story.

Given the strong nexus between traditional bullying and bullying online, we have partnered with the Yale Center for Emotional Intelligence to create our Bullying Prevention Hub, available at https://www.facebook.com/safety/bullying. This is a resource for teens, parents and educators seeking support and help for issues related to bullying and other conflicts. It offers step-by-step plans, including guidance on how to start some important conversations for people being bullied, parents who have had a child being bullied or accused of bullying, and educators who have had students involved with bullying.

We also may take additional enforcement action against violating accounts, including deactivation. Additionally, enforcement of our authentic identity policy has been effective in combatting bullying on our platform as we know that when people do not use their authentic identity on Facebook they are five times more likely to violate our policies.

We also offer have a Safety Center available in over 60 languages. Approximately 80,000 to 100,000 people visit our Safety Center every month where they can obtain guidance and expert advice on online safety and prevention of bullying.

We also support on-the-ground online safety and anti-bullying programs, including research-based, outcome-tested peer-to-peer programming and a social and emotional learning initiative to give students the skills they need to create supportive communities free from bullying. We do this because we believe having these skills offline is connected to having them online and will have long term impact on how people behave online. That said, we work continuously with over 250 online safety organizations worldwide to make our platform safer and more secure, and our effort to do so is a holistic one that involves adding resources when issues arise and a continual evaluation of our processes and policies.

13. At the House hearing, Congressman Rush asked about steps Facebook is taking to ensure that the targeted advertising on Facebook complies with federal laws, such as the Civil Rights Act of 1968. You responded that Facebook removed the option for advertisers to exclude ethnic groups from advertising.

a. Please expand on that. What other steps are you taking to ensure advertising on Facebook is compliant with federal anti-discrimination laws?

b. What actions is Facebook taking to ensure compliance with the Fair Housing Act?

c. Many concerns have also been raised about Facebook's targeted advertising allowing employers advertising jobs to show those ads only to younger workers and therefore allowing age discrimination. What actions is Facebook taking to ensure that its targeted advertising does not facilitate age discrimination in violation of the Age Discrimination in Employment Act?

d. What actions is Facebook taking to prevent discrimination against other protected classes, such as religion, sex, and familial status?

Our Terms and Advertising Policies have long emphasized our prohibition on the use of Facebook's platform to engage in wrongful discrimination. Starting in late 2016, we began implementing additional protections for the people who use Facebook. Specifically, we set out to help better educate advertisers about our policies against discrimination and relevant federal and state laws, and to help prevent the abuse of our tools. First, we updated our Advertising Policies applicable to all advertisers and advertisements to strengthen our prohibition against discrimination, and we added a section to provide advertisers with anti-discrimination educational resources from government agencies and civil rights groups. Second, we implemented technical measures aimed at better protecting users from wrongful discrimination by advertisers that offer housing, employment and credit opportunities. We continue to work to improve these measures.

We are continuing to evaluate the targeting options we make available to advertisers. This work involves consultation with key stakeholders outside the company, including with policymakers, regulators, civil rights experts, and consumer advocates. The decision to remove

targeting options is not something we take lightly: as many of these stakeholders have pointed out, targeting is a key mechanism for forging meaningful connections between people and organizations on Facebook.

One recent example illustrates the challenge of getting this work right. Earlier this year, we eliminated the ability to target people based on the "interested in" field that people can add to their Facebook profiles. People can indicate that they are interested in men, women, or both, and some consider the field to be a place where people can indicate their sexual orientation. After receiving feedback from a range of stakeholders, we eliminated the ability to target based on this field. Although some groups applauded the decision, others criticized it, noting that it would now be harder to reach certain groups.

We also are working to provide more in-product education about advertisers' obligations under our non-discrimination policy, and anticipate that this education will be more detailed and will be presented to a broader range of advertisers than our current education. We just launched globally View Active Ads, a feature that will enable anyone to see all of the ads an advertiser is currently running by visiting the advertiser's Facebook Page. This level of transparency is unprecedented among advertising platforms, and we believe it will further our efforts to combat discrimination by giving people the opportunity to see ads regardless of whether they are in the target audience.

We have focused on measures that are designed to prevent advertisers from misusing our tools to place discriminatory housing, credit and employment ads, including: requiring such advertisers to certify their compliance with our Advertising Policies and with relevant anti-discrimination laws and prophylactically removing advertisers' ability to use certain categories of information to target their audience. Some of these measures are proactive, such as the classifiers we use to detect when an advertiser is attempting to run a housing, credit, or employment ad. Facebook rejects ads from advertisers who do not certify compliance. We also recently launched automated tools to proactively identify racist or offensive content and hate speech in ads.

In addition, Facebook conducts an automated review of ads to ensure that they do not assert or imply personal attributes in violation of our Advertising Policies. Ads that violate this policy are rejected. Advertisers can appeal these rejections. Understanding that we might not be able to prevent every misuse of our ad tools, we encourage users to report offensive ads to Facebook. Ads that violate our Advertising Policies are removed when we become aware of them. We also anticipate that the View Ads tool—which, as described above, will allow people to see all the ads an advertiser is currently running—will encourage people to report more ads to us, and will therefore enhance our efforts to curtail misuse of our tools.

The Honorable John Sarbanes

1. Political and Issue Ad Disclosure

a. In October 2017, Facebook announced that political ads placed on Facebook would soon be subject to heightened transparency requirements.[1] In addition to implementing a more stringent verification process for purchasers, your team announced that political ads would soon carry disclaimers stating who paid for them and making it easier for viewers to see the ads that a given account is running. This new policy was to be beta tested in Canadian markets before being implemented in the United States "ahead of the US midterm elections."[2]

i Given that U.S. midterm campaigns are already underway, with two states already having had their primary elections and twelve more set for their primaries in the month of May, when will this new policy go into effect? Please provide internal documents that describe the policy and the planned roll-out in the United States.

ii On April 6, 2018, Facebook announced that this new verification and disclosure regime will also include so-called "issue ads" and, in doing so, endorsed the Honest Ads Act.[3] In your view, should Congress pass the Honest Ads Act as is? If not, why?

b. Facebook officials admit that this new political and issue ad regime will not be perfect, recognizing that some ads that violate its policy—whether due to verification concerns or content violations—may evade initial detection. Your legislative affairs team has said Facebook plans to have a "reactive" policy of pulling down content after it is determined to violate its terms of service.

i Under the new ad regime, if an ad is taken down, will Facebook notify users who engaged with content that was later removed from the platform?

ii Technologically, could you notify users who engaged with content that was later taken down? If so, will you provide such notification? If not, please explain.

We now require that advertisers clearly label all election-related and issue ads on Facebook and Instagram in the US—including a "Paid for by" disclosure from the advertiser at the top of the ad. This will help people see who is paying for the ad—which is especially

[1] Rob Goldman, *Update on Our Advertising Transparency and Authenticity Efforts*, FACEBOOK (October 27, 2017) (online at https://newsroom.fb.com/news/2017/10/update-on-our-advertismg-transparency-and- authenticity-efforts/).
[2] *Id*.
[3] Griffin Connolly, *Facebook To Tighten Grip On Political Ads, As Zuckerberg Heads To Hill*, ROLL CALL (April 6, 2018) (online at www.rollcall.com/news/politics/facebook-political-ads-zuckerberg-hill).

important when the Page name doesn't match the name of the company or person funding the ad. For more information, see https://newsroom.fb.com/news/2018/04/transparent-ads-and-pages/.

When people click on the label, they'll be taken to an archive with more information. For example, we'll provide the campaign budget associated with an individual ad and how many people saw it—including aggregated information about their age, location and gender. That same archive can be reached at https://www.facebook.com/politicalcontentads. People on Facebook visiting the archive can see and search ads we've identified with political or issue content that an advertiser has run in the US for up to seven years.

Advertisers wanting to run ads with political content in the US will need to verify their identity and location. More information is available at https://newsroom.fb.com/news/2018/04/transparent-ads-and-pages/. Enforcement of these new features and the Political Ads policy, available at https://www.facebook.com/policies/ads/restricted_content/political, began on May 24.

We're closely monitoring developments in Congress, including proposed legislation like the Honest Ads Act. Our policy reflects language from existing laws as well as proposed laws. But, we're not waiting. We've been hearing calls for increased transparency around ads with political content for some time now. We've taken the first steps toward providing that transparency, and we hope others follow.

2. Trending Topics

a. Facebook's Trending Topics section "helps people discover timely and relevant conversations about the news that they care about." For years, this section has relied on human editors to curate content by filtering out inappropriate content or content that offends Facebook's community standards.

In 2016, after reported lobbying by conservative political leaders, Congressional Republicans, and supporters of then-candidate Donald Trump who accused Facebook's Trending Topics editors of "anti-conservative political bias," Facebook removed the human editors from their Trending Topics section and replaced them with an algorithm, in the run-up to the 2016 election.[4]

i Please explain, in detail, the process by which Facebook decided to remove human editors from the Trending Topics section and provide any documents, meeting notes, or memoranda relating to the decision.

[4] Allana Akhtar, *Facebook Removes Human-Written Descriptions on Trending Topics*, USA TODAY (August 26, 2016) (online at www.usatoday.com/story/tech/news/2016/08/26/facebook-removes-human-written-descriptions-trending-topics/89440416/).

ii **It has been reported that conservative activists visited Facebook's headquarters to lobby for the removal of human editors.[5] Who within Facebook or its board advocated for their visit? Please provide any documents, meeting notes, or memoranda relating to the deliberation.**

iii **Was there a comparable effort to bring liberal or non-partisan activists to Facebook headquarters to hear their concerns about fake news and propaganda being spread on Facebook's platform?**

iv **Was the Trending Topics algorithm, at any time, effectively gamed by organizations intent on spreading fake news and propaganda? Would the human editors have been vulnerable in this way? If so, how?**

v **Do you draw any connection between the decision to remove the editors and the subsequent spread of Russian-originated and other fake news intended to influence the outcome of the election? If not, why?**

vi **Given that the decision to remove the editors seems to have contributed to the ease with which Fake news could influence the election, are you considering any steps to reinstate human editors? If not, why?**

Earlier this month, we announced plans to remove Trending to make way for future news experiences on Facebook. We introduced Trending in 2014 as a way to help people discover news topics that were popular across the Facebook community. However, it was only available in five countries and accounted for less than 1.5 percent of clicks to news publishers on average. We determined through research that over time people found the product to be less and less useful. In line with our announcement earlier this month, we have removed Trending from Facebook.

Being a platform for all ideas is a foundational principle of Facebook. We are committed to ensuring there is no bias in the work we do. Suppressing content on the basis of political viewpoint or preventing people from seeing what matters most to them is directly contrary to Facebook's mission and our business objectives.

When allegations of political bias surfaced in relation to Facebook's Trending Topics feature, we immediately launched an investigation to determine if anyone violated the integrity of the feature or acted in ways that are inconsistent with Facebook's policies and mission. We spoke with current reviewers and their supervisors, as well as a cross-section of former reviewers; spoke with our contractor; reviewed our guidelines, training, and practices; examined the effectiveness of operational oversight designed to identify and correct mistakes and abuse; and analyzed data on the implementation of our guidelines by reviewers.

---

[5] Nicholas Thompson & Fred Vogelstein, *Inside The Two Years That Shook Facebook—And The World*, WIRED (February 12, 2018) (online at www.wired.com/story/inside-facebook-mark-zuckerberg-2-years-of-hell/).

Ultimately, our investigation revealed no evidence of systematic political bias in the selection or prominence of stories included in the Trending Topics feature. In fact, our analysis indicated that the rates of approval of conservative and liberal topics are virtually identical in Trending Topics. Moreover, we were unable to substantiate any of the specific allegations of politically-motivated suppression of subjects or sources, as reported in the media. To the contrary, we confirmed that most of those subjects were in fact included as trending topics on multiple occasions, on dates and at intervals that would be expected given the volume of discussion around those topics on those dates.

Nonetheless, as part of our commitment to continually improve our products and to minimize risks where human judgment is involved, we are making a number of changes:

- We have engaged an outside advisor, former Senator Jon Kyl, to advise the company on potential bias against conservative voices. We believe this external feedback will help us improve over time and ensure we can most effectively serve our diverse community and build trust in Facebook as a platform for all ideas.

- We continue to expand our list of outside partner organizations to ensure we receive feedback on our content policies from a diverse set of viewpoints.

- We have made our detailed reviewer guidelines public to help people understand how and why we make decisions about the content that is and is not allowed on Facebook.

- We have launched an appeals process to enable people to contest content decisions with which they disagree.

- We are instituting additional controls and oversight around the review team, including robust escalation procedures and updated reviewer training materials.

These improvements and safeguards are designed to ensure that Facebook remains a platform for all ideas and enables the broadest spectrum of free expression possible.

3. Political Sales Support, Campaign Finance Law, and the Influence Economy

a. Facebook provides so-called "sales support" teams for their clients, including political clients. However, federal campaign finance law is clear that providing staff or assistance to a political campaign in a manner outside the normal course of business or on better terms than offered to commercial clients can constitute an illegal contribution to the campaign, violating so-called "in-kind" contribution limits designed to prevent quid pro quo corruption.

i What parameters are used to determine when a political client is offered "sales support" to assist with advertising on Facebook, as both the Trump and Clinton campaigns were reported to have been offered? Please provide documents and communications referring or

relating to how "sales support" representatives are offered to political campaigns.

ii **When were these offers made to the Trump and Clinton campaigns? What specific assistance was offered? What, if any, limitations were put on the offer? What was accepted by each campaign? Please provide any documents or communications regarding assistance offered to or accepted by the campaigns, including but not limited to written offer terms and any subsequent written offer terms provided by Facebook to the political campaigns detailing the services that would—or could—be rendered.**

iii **Did the offers differ in any way? Did either the Trump or Clinton campaign negotiate the terms of the offer, including requesting or refusing specific employees?**

iv **Were any "sales support" teams "embedded"—or domiciled—in a given campaign's operation? How frequently did the "sales support" teams visit either campaign's physical operation?**

v **Did the campaigns pay for this assistance beyond the cost of the ad buys? If so, did it cover Facebook's full cost in providing the services?**

We want all candidates, groups, and voters to use our platform to engage in elections. We want it to be easy for people to find, follow, and contact their elected representatives—and those running to represent them. That's why, for candidates across the political spectrum, Facebook offers the same levels of support in key moments to help campaigns understand how best to use the platform.

Facebook representatives advise political advertisers on Facebook, as they would with other, non-political managed accounts. During the 2016 election cycle, Facebook worked with campaigns to optimize their use of the platform, including helping them understand various ad formats and providing other best practices guidance on use of the platform.

No one from Facebook was assigned full-time to the Trump campaign, or full-time to the Clinton campaign. We offered identical support to both the Trump and Clinton campaigns, and had teams assigned to both. Everyone had access to the same tools, which are the same tools that every campaign is offered. The campaigns did not get to "hand pick" the people who worked with them from Facebook. Both campaigns approached things differently and used different amounts of support.

We continuously work to ensure that we comply with all applicable laws and policies. We have a compliance team that trains our sales representatives to comply with all federal election law requirements in this area. Facebook employees are encouraged to raise any concerns about improper activity to their managers. While our investigation is ongoing, our review indicates that Facebook employees did not identify any issues involving the improper use of

Facebook data in the course of their interactions with Cambridge Analytica during the 2016 US Presidential campaign.

In general, political data firms working on the 2016 campaign had access to Facebook's advertising support services, including technical support, and best practices guidance on how to optimize their use of Facebook. Everyone had access to the same tools, which are the same tools that every campaign is offered, and is consistent with support provided to commercial clients in the normal course of business.

b. It has been reported that the Trump campaign accepted the paid Facebook employees to serve as "campaign embeds." Reporting indicates these individuals played a central role in the Trump campaign, supporting the Trump communication operation in ways that extended far beyond helping the campaign use Facebook's tools to target ads, including by "actively shaping campaign communications through their close collaboration with political staffers."[6] It was reported that the "sales support" officers were enmeshed with the Trump campaign and helped "to tee up responses to likely lines of attack during debates."[7] In contrast, the Clinton campaign was reported to have "viewed [Facebook] as vendors rather than consultants."[8]

i Did the services rendered to the respective campaigns differ in any way? If so, how and why? Please provide any documents, meeting notes, or memoranda relating to how "sales support" supported each given campaign, with an enumerated list of known services rendered.

ii Were the "sales support" officers instructed to assist in developing media strategy for the candidates? What did Facebook expect these employees to do for the campaigns? Did Facebook make any other special services available to the campaign that extended beyond helping the campaign target its ads?

iii Who at Facebook determined the work "sales support" officers would do? Were the "sales support" officers for either campaign overseen by Facebook executives in any way?

iv How do you, as CEO, know what work they did for the campaigns? Did they report to Facebook on the work they were doing? If so, how frequent was said reporting? Please provide any documents, meeting

---

[6] Nancy Scola, *How Facebook, Google and Twitter 'Embeds' Helped Trump in 2016*, Politico (October 26, 2017) (online at www.politico.com/story/2017/10/26/facebook-google-twitter-trump-244191). *See also* Daniel Kreiss & Shannon McGregor, *Technology Finns Shape Political Communication: The Work of Microsoft, Facebook, Twitter, and Google With Campaigns During the 2016 U.S. Presidential Cycle*, POLITICAL COMMUNICATION (October 26, 2017) (online at www.tandfonline.com/doi/full/10.1080/10584609.2017.1364814).

[7] *Id.*

[8] *Supra* 7.

notes, or memoranda relating to executive-level oversight of the political "sales support" teams.

v **What safeguards, if any, did Facebook implement to ensure that the services and staff it provided were not illegal corporate contributions? What steps, if any, does Facebook have planned to institute additional safeguards? Does Facebook plan to continue to provide "campaign embeds" to political campaigns? Please provide any training documents, service agreements, meeting notes, or memoranda relating to how political "sales support" teams are training.**

vi **Did Facebook or any Facebook employees working as "sales support" officers grant any special approval rights or services to either campaign? What safeguards or monitoring are in place to avoid such illicit behavior?**

See Response to Question 3(a).

4. Facebook's Expectations for the 2018 Election Cycle

a. A grand jury has indicted 13 Russian nationals for activities that relied upon Facebook as both an advertising platform and social network. Some have raised concerns that the News Feed reforms that you announced recently—including the idea that Facebook will put a renewed premium on content from family, friends, and network contacts over legitimate news—may exacerbate the effectiveness of the tactics deployed by Russia operatives during the 2016 election cycle, given their use of organic Facebook groups and content generation.

i **How is Facebook working to mitigate such a scenario? Please provide documents, meeting notes, or memoranda relating to how Facebook is ensuring the News Feed reforms do not inadvertently amplify illicit foreign campaign content.**

In the run-up to the 2016 elections, we were focused on the kinds of cybersecurity attacks typically used by nation states, for example phishing and malware attacks. And we were too slow to spot this type of information operations interference. Since then, we've made important changes to prevent bad actors from using misinformation to undermine the democratic process.

This will never be a solved problem because we're up against determined, creative and well-funded adversaries. But we are making steady progress. Here is a list of the 10 most important changes we have made:

- **Ads transparency.** Advertising should be transparent: users should be able to see all the ads an advertiser is currently running on Facebook, Instagram and Messenger. And for ads with political content, we've created an archive that will hold ads with political content for seven years—including information about ad impressions and spend, as well as demographic data such as age, gender and location. People in Canada and Ireland have

already been able to see all the ads that a Page is running on Facebook—and we've launched this globally.

- **Verification and labeling.** Every advertiser will now need to confirm their ID and location before being able to run any ads with political content in the US. All ads with political content will also clearly state who paid for them.

- **Updating targeting.** We want ads on Facebook to be safe and civil. We thoroughly review the targeting criteria advertisers can use to ensure they are consistent with our principles. As a result, we removed nearly one-third of the targeting segments used by the IRA. We continue to allow some criteria that people may find controversial. But we do see businesses marketing things like historical books, documentaries or television shows using them in legitimate ways.

- **Better technology.** Over the past year, we've gotten increasingly better at finding and disabling fake accounts. We now block millions of fake accounts each day as people try to create them—and before they've done any harm. This is thanks to improvements in machine learning and artificial intelligence, which can proactively identify suspicious behavior at a scale that was not possible before—without needing to look at the content itself.

- **Action to tackle fake news.** We are working hard to stop the spread of false news. We work with third-party fact-checking organizations to limit the spread of articles rated false. To reduce the spread of false news, we remove fake accounts and disrupt economic incentives for traffickers of misinformation. We also use various signals, including feedback from our community, to identify potential false news. In countries where we have partnerships with independent third-party fact-checkers, stories rated as false by those fact-checkers are shown lower in News Feed. If Pages or domains repeatedly create or share misinformation, we significantly reduce their distribution and remove their advertising rights. We also want to empower people to decide for themselves what to read, trust, and share. We promote news literacy and work to inform people with more context. For example, if third-party fact-checkers write articles about a news story, we show them immediately below the story in the Related Articles unit. We also notify people and Page Admins if they try to share a story, or have shared one in the past, that's been determined to be false. In addition to our own efforts, we're learning from academics, scaling our partnerships with third-party fact-checkers and talking to other organizations about how we can work together.

  A key focus is working to disrupt the economics of fake news. For example, preventing the creation of fake accounts that spread it, banning sites that engage in this behavior from using our ad products, and demoting articles found to be false by fact checkers in News Feed—causing it to lose 80% of its traffic. We now work with independent fact checkers in the US, France, Germany, Ireland, the Netherlands, Italy, Mexico, Colombia, India, Indonesia and the Philippines with plans to scale to more countries in the coming months.

- **Significant investments in security.** We're doubling the number of people working on safety and security from 10,000 last year to over 20,000 this year. We expect these investments to impact our profitability. But the safety of people using Facebook needs to come before profit.

- **Industry collaboration.** Recently, we joined 34 global tech and security companies in signing a TechAccord pact to help improve security for everyone.

- **Information sharing and reporting channels.** In the 2017 German elections, we worked closely with the authorities there, including the Federal Office for Information Security (BSI). This gave them a dedicated reporting channel for security issues related to the federal elections.

- **Tracking 40+ elections.** In recent months, we've started to deploy new tools and teams to proactively identify threats in the run-up to specific elections. We first tested this effort during the Alabama Senate election, and plan to continue these efforts for elections around the globe, including the US midterms. Last year we used public service announcements to help inform people about fake news in 21 separate countries, including in advance of French, Kenyan and German elections.

- **Action against the Russia-based IRA.** In April, we removed 70 Facebook and 65 Instagram accounts—as well as 138 Facebook Pages—controlled by the IRA primarily targeted either at people living in Russia or Russian-speakers around the world including from neighboring countries like Azerbaijan, Uzbekistan and Ukraine. The IRA has repeatedly used complex networks of inauthentic accounts to deceive and manipulate people in the US, Europe and Russia—and we don't want them on Facebook anywhere in the world.

ii What is your greatest concern as it relates to Facebook's vulnerabilities to malicious use in our political system as we enter the 2018 midterm election season?

See Response to Question 4(i).

iii How can Congress support your efforts to harden our defenses against future malicious political activity occurring on Facebook?

We agree that information sharing among companies and government is critical to combating constantly evolving cyber threats. We have been working with many others in the technology industry, including Google and Twitter, on this issue, building on our long history of working together on issues like child safety and counterterrorism. We also have a history of working successfully with the DOJ, the FBI, and other law enforcement to address a wide variety of threats to our platform, and we look forward to continuing to work with law enforcement and government on these issues.

The Honorable Jerry McNerney

1. After clarifying with your team at the hearing, you stated in your oral testimony that "web logs are not in Download Your Information." Does Facebook plan to make users' web browsing history a part of Download Your Information? If so, when will this feature be available?

Our Download Your Information or "DYI" tool is Facebook's data portability tool and was launched many years ago to let people access and download many types of information that we maintain about them. The data in DYI and in our Ads Preferences tool contain each of the interest categories that are used to show people ads, along with information about the advertisers that are currently running ads based on their use of an advertiser's website or app. People also can choose not to see ads from those advertisers. We recently announced expansions to Download Your Information, which, among other things, will make it easier for people to see their data, delete it, and easily download and export it. More information is available at https://newsroom.fb.com/news/2018/04/new-privacy-protections/.

Responding to feedback that we should do more to provide information about websites and apps that send us information when people use them, we also announced plans to build Clear History. This new feature will enable users to see the websites and apps that send us information when they use them, clear this information from their account, and turn off Facebook's ability to store it associated with their account going forward.

It will take a few months to build Clear History. We'll work with privacy advocates, academics, policymakers, and regulators to get their input on our approach, including how we plan to remove identifying information and the rare cases where we need information for security purposes. We've already started a series of roundtables in cities around the world and heard specific demands for controls like these at a session we held at our headquarters. We're looking forward to doing more.

We have also introduced Access Your Information. This feature provides a new way for people to access and manage their information. Users can go here to delete anything from their timeline or profile that they no longer want on Facebook. They can also see their ad interests, as well as information about ads they've clicked on and advertisers who have provided us with information about them that influence the ads they see. From here, they can go to their ad settings to manage how this data is used to show them ads.

Apps and websites that use features such as the Like button or Facebook Analytics send us information to make their content and ads better. We also use this information to make user experience on Facebook better. If a user clears his or her history or uses the new setting, we'll remove identifying information so a history of the websites and apps the user used won't be associated with the user's account. We'll still provide apps and websites with aggregated analytics—for example, we can build reports when we're sent this information so we can tell developers if their apps are more popular with men or women in a certain age group. We can do this without storing the information in a way that's associated with the user's account, and as always, we don't tell advertisers who users are.

2. You also stated in your oral testimony that Facebook stores users' web logs "temporarily." How long does Facebook store this information? Please specify the period of time. If this answer varies depending on the website accessed, please explain why this is the case and note any differences in the duration of time for which this information is stored.

Facebook receives log data when websites and advertisers use our technologies such as our social plug-in and the Facebook pixel. The amount of time we retain this information depends on the specific data. For example, logs relating to social plug-ins on third-party websites can be from registered users or from non-registered people without a Facebook account. Logs for social plug-ins visited by users is retained for 90 days before they are aggregated. For non-users, these individual logs are stored for 10 days. Advertiser data sent to us through the Facebook pixel is retained for 180 days.

Facebook Analytics is a product that enables website publishers to understand how people use their websites. Facebook analytics stores web log data for up to two years to help provide publishers with general statistics about how usage of their sites changes over time—for example, comparing usage in one month to usage in the same month during the preceding year.

Responding to feedback that we should do more to provide information about websites and apps that send us information when people use them, we have announced plans to build Clear History. This new feature will enable users to see the websites and apps that send us information when they use them, clear this information from their account, and turn off Facebook's ability to store it associated with their account going forward.

3. You further stated in your oral testimony that Facebook converts the web logs into a set of ad interests and that this information is included in Download Your Information. How far back in a user's history is the user able to access this information?

Our Download Your Information or "DYI" tool is Facebook's data portability tool and was launched many years ago to let people access and download many types of information that we maintain about them. The data in DYI and in our Ads Preferences tool contain each of the interest categories we store at the time of the download request that are used to show people ads, along with information about the advertisers that are currently running ads based on their use of an advertiser's website or app. People also can choose not to see ads from those advertisers. We recently announced expansions to Download Your Information, which, among other things, will make it easier for people to see their data, delete it, and easily download and export it. More information is available at https://newsroom.fb.com/news/2018/04/new-privacy-protections/.

Through Ad Preferences, people are able to see the range of ad interests currently associated with their account. These interests may change over time if people remove them or if we make changes to the interests we offer through our ads tools. People can also customize their advertising experience by removing interests that they do not want to inform the Facebook ads they see.

Responding to feedback that we should do more to provide information about websites and apps that send us information when people use them, we also announced plans to build Clear History. This new feature will enable users to see the websites and apps that send us information when they use them, clear this information from their account, and turn off Facebook's ability to store it associated with their account going forward.

4. Why is the information listed under Your Categories in Ad Preferences not included as part of Download Your Information? Does Facebook plan to include it?

See Response to Question 1.

5. Are there any categories that Facebook uses to help advertisers reach people, but are not currently listed under Your Categories in Ad Preferences? If so, please specify the categories and note any plans that Facebook has to make this information available to its users.

As explained in our Data Policy, we collect three basic categories of data about people: (1) data about things people do and share (and who they connect with) on our services, (2) data about the devices people use to access our services, and (3) data we receive from partners, including the websites and apps that use our business tools. Our Data Policy provides more detail about each of the three categories.

We use data from each of the categories described above to obtain these interests and to personalize every aspect of our services, which is the core value we offer and the thing that makes Facebook services unique from other online experiences. This includes selecting and ranking relevant content, including ads, posts, and Page recommendations, to cite but a few examples.

For example, we use the data people provide about their age and gender to help advertisers show ads based on those demographics but also to customize the pronouns on our site and deliver relevant experiences to those users.

We use data about things people do on Facebook, such as the Pages they like, to associate "interests" with their accounts, so we can rank posts relating to those interests higher in NewsFeed, for example, or enable advertisers to reach audiences—i.e., groups of people—that share those interests. For example, if a person has liked Pages about baseball, we might associate them with interests called "baseball" or "sports."

We use data from devices (such as location data) to help advertisers reach people in particular areas. For example, if people have shared their device locations with Facebook or checked into a specific restaurant, we can show them organic posts from friends who have been in that location or we can show them ads from an advertiser that wants to promote its services in their area or from the restaurant.

We also help advertisers reach people who have given the advertiser their contact information or who have used the advertiser's website or app. For example, advertisers can send us a hashed list of email addresses of people they would like to reach on Facebook. If we have

matching email addresses, we can show those people ads from that advertiser (although we cannot see the email addresses which are sent to us in hashed form, and these are deleted as soon as we complete the match).

Again, for people who are new to Facebook, we may have minimal data that we can use to personalize their experience, including their News Feed, their recommendations and the content (organic and sponsored) that they see. For people who have used our services for longer, we likely have more data, but the amount of data will depend on the nature of that use and how they have used our controls.

In addition to general controls—such as Activity Log—we provide controls that specifically govern the use of data for ads. Through Ad Preferences, people see and control things like: (1) their "interests," which are keywords associated with a person based on activities such liking Pages and clicking ads; (2) their "behaviors" (which we also call "categories"), which generally reflect how, when and where they connect to Facebook; and (3) the advertisers that are currently showing them ads based on the person's contact information, based on the person's previous use of the advertiser's website or app, or based on a visit to the advertiser's store. People also can choose whether we use information about their activities on websites and apps off of Facebook to show them ads through Facebook, and whether we can use their Facebook advertising interests to show them ads off of Facebook. People's use of these controls will, of course, affect the data we use to show them ads.

6. Does Download Your Information include all of the location information, including GPS location information, about a user that Facebook has obtained from the user or from any other party? If not, please specify all of the location information that is not included in Download Your Information and whether Facebook plans to include this information.

See Response to Question 1.

7. Does Download Your Information include all of the information that Facebook obtains about its users from third-party apps? If not, please specify what information is not included and whether Facebook plans to include this information.

See Response to Question 1.

8. Does Download Your Information include information that Facebook collects about the apps that its users visit and users' activities within those apps? If not, please specify what information is not included and whether Facebook plans to include this information.

See Response to Question 1.

9. If a user clears his or her search history from Facebook, does Facebook retain the information that was cleared? If so, does Facebook plan to include the information that was cleared in Download Your Information?

See Response to Question 1.

Our policies limit our retention of the data that we receive in several ways. Specifically, we store data until it is no longer necessary to provide our services and Facebook products, or until a person's account is deleted—whichever comes first. This is a case-by-case determination that depends on things like the nature of the data, why it is collected and processed, and relevant legal or operational retention needs. If a user posts something on their Facebook profile, then that information would be retained until they delete it or until they delete their account.

We also have other policies that are designed to limit our retention of other types of information about people. For example, if a user clicks a "Like" button that appears on a third-party site, we may use that information to show the person a more personalized experience on Facebook, to help maintain and improve our service, and to protect both the user and Facebook from malicious activity. We delete or anonymize the URL where the Like occurred within 90 days.

In general, when a user deletes their account, we delete things they have posted, such as their photos and status updates, and they won't be able to recover that information later. (Information that others have shared about them isn't part of their account and won't be deleted.)

There are some limited exceptions to these policies: For instance, information can be accessed and preserved for an extended period when it is the subject of a legal request or obligation, governmental investigation, or investigations of possible violations of our terms or policies, or otherwise to prevent harm. We also retain information from accounts disabled for terms violations for at least a year to prevent repeat abuse or other term violations.

Particularly in the past few months, we've realized that we need to take a broader view of our responsibility to our community. Part of that effort is continuing our ongoing efforts to identify ways that we can improve our privacy practices. This includes restricting the way that developers can get information from Facebook and announcing plans to build Clear History, a new feature that will enable users to see the websites and apps that send us information when they use them, clear this information from their accounts, and turn off our ability to store it associated with their accounts going forward.

10. What information does Instagram obtain about its users, whether this information is collected directly from the user or from a third party, that is not included in Instagram's Data Download tool? Please specify the nature of the information (e.g., search history, location data, web browsing history, apps that its users access and activity in those apps, etc.), and any plans to include this information in the Data Download tool.

Our Instagram Data Policy describes the data we collect and is available at https://help.instagram.com/519522125107875.

11. On what date will Facebook users in the United States have the same controls and settings as users in the European Union?

We provide the same tools for access, rectification, erasure, data portability and others to people in the US (and globally) that we provide in the European Union, and many of those tools (like our Download Your Information tool, Ad Preferences tool, and Activity Log) have been available globally for many years. We have recently begun providing direct notice of these controls and our updated terms of service to people around the world (including in the US), allowing people to choose whether or not to enable or disable these settings or to consent to our updated terms. The controls and settings that Facebook is enabling as part of GDPR are available to people around the world, including settings for controlling our use of face recognition on Facebook and for controlling our ability to use data we collect off Facebook Company Products to target ads.

12. Once the changes are made to the settings and controls for users in the United States, will there be any differences between the options within these settings and controls that users are given in the United States versus the options that users are given in the European Union? Please specify the differences.

The GDPR requires companies to obtain explicit consent to process certain kinds of data ("special categories of data" like biometric data). We are seeking explicit consent from people in Europe to three specific uses of data: facial recognition data (which previously was not enabled in Europe), special categories of data and use of data we collect off Facebook Company Products to target ads. We recently began providing direct notice of these controls and our updated terms to people around the world (including in the US), allowing people to choose whether or not to enable or disable these settings or to agree to our updated terms. Outside of Europe we are not requiring people to complete those flows if they repeatedly indicate that they do not want to go through the experience. At the same time, the events of recent months have underscored how important it is to make sure people know how their information is used and what their choices are. So, we decided to communicate prominently on Facebook—through a full-screen message and a reminder to review at a later date. People can choose to dismiss or ignore these messages and continue using Facebook.

The controls and settings that Facebook is enabling as part of GDPR are already available to other users around the world, including in the US. We also provide identical levels of transparency in our user agreements and in product notices to people in the US that we are providing under GDPR.

In the US, where these settings are already in place, people will have a mechanism to maintain their current choice or to change it. In each of these cases, we want people to make the choice—not Facebook—so nobody's settings will change as part of this roll out unless they choose to change an existing setting.

And we also provide the same tools for access, rectification, erasure, data portability and others to users in in the US and rest of world that we provide in Europe, and many of those tools (like our Download Your Information tool, Ads Preferences tool, and Activity Log) have been available globally for many years.

13. Will there be any differences between how the settings and controls and the options within the settings and controls are laid out for users in the United States versus for users in the European Union? Please specify the differences.

See Response to Question 12.

We are seeking explicit consent from people in Europe to three specific uses of data: facial recognition data (which previously was not enabled in Europe), special categories of data, and use of data we collect off Facebook Company Products to target ads. We recently began providing direct notice of these controls and our updated terms to people around the world (including in the US), allowing people to choose whether or not to enable or disable these settings or to agree to our updated terms. Outside of Europe we are not requiring people to complete those flows if they repeatedly indicate that they do not want to go through the experience. At the same time, the events of recent months have underscored how important it is to make sure people know how their information is used and what their choices are. So, we decided to communicate prominently on Facebook—through a full-screen message and a reminder to review at a later date. People can choose to dismiss or ignore these messages and continue using Facebook.

GDPR does not require consent for most uses of personal information, and instead, recognizes that many uses of data are necessary to provide a service or within companies' legitimate interests or the public interest. We agree that different levels of consent or notice are appropriate depending on the type of information or contemplated use at issue.

14. It has been observed that social media platforms, such as Facebook and Instagram, tend to engage users in excessive screen time as opposed to in-person social interactions. Is Facebook conducting any research related to this phenomenon? If so, when will this research be available and how will it be used? Will you make the results of that research available to Congress and the public?

Research shows that strengthening our relationships improves our well-being and happiness. But recently we've gotten feedback from our community that public content—posts from businesses, brands and media—is crowding out the personal moments that lead us to connect more with each other. So we've studied this trend carefully by looking at the academic research and doing our own research with leading experts at universities. The research shows that when we use social media to connect with people we care about, it can be good for our well-being. On the other hand, passively reading articles or watching videos—even if they're entertaining or informative—may not be as good. Based on this, we're making a major change to how we build Facebook. We are changing the goal for our product teams from focusing on helping users find relevant content to helping them have more meaningful social interactions.

The Honorable Ben Ray Luján

1. **Worst-Case Scenario Planning: In your testimony, you referred to Facebook as an "idealistic and optimistic company" and suggested that Facebook didn't have a "broad enough" view of its responsibility.**

   a. **Do you believe that your competitors and the other companies who trade in personal information share Facebook's idealism and optimism?**

   b. **Do you trust your competitors to behave appropriately without stronger consumer safeguards and protections?**

   c. **Does Facebook employ anyone whose job it is to crisis plan or think through worst-case scenarios?**

   d. **If yes, how often do they discuss their findings and recommendations with Facebook's leadership?**

   e. **Would Facebook consider employing an ombudsman in the way other media companies do to hold itself accountable and to better understand its responsibilities?**

We believe strongly in providing meaningful privacy protections to people. This is why we work hard to communicate with people about privacy and build controls that make it easier for people to control their information on Facebook. For example, Facebook has redesigned its settings menu to make things easier to find and introduced new Privacy Shortcuts. These shortcuts allow users to make their account more secure, control their personal information, control which ads they see, and control who sees their posts and profile information. Facebook has also introduced additional tools to find, download, and delete user data.

We've worked with regulators, legislators, and privacy experts, at both the state and national levels to educate people and businesses about privacy. We believe an important component of any privacy regulation is clear and consistent oversight and enforcement. We intend to continue this collaborative work to promote privacy protections for our community.

Facebook is generally not opposed to regulation but wants to ensure it is the right regulation. The issues facing the industry are complex, multi-faceted, and affect an important part of peoples' lives. As such, Facebook is absolutely committed to working with regulators, like Congress, to craft the right regulations. Facebook would be happy to review any proposed legislation and provide comments.

2. **Malicious Actors: Facebook recently announced that one of the platform's search features allowed "malicious actors" to scrape data on virtually all of Facebook's two billion users.**

   a. **Please explain what Facebook means by "malicious actors."**

   b. **What could these malicious actors do with this data?**

c. Did your company debate the wisdom of this feature and how it could be misused before it was rolled out?

d. If consumers are harmed by the collection of this data, what, if anything, will Facebook do to make people whole?

e. When did Facebook understand that this feature could be misused? Why did you wait so long to act?

f. As Facebook rolls out new features, is anyone asked to consider how these features could be misused? If so, who?

In April, we found out that a feature that lets users look someone up by their phone number and email may have been misused by browsers looking up people's profiles in large volumes with phone numbers they already had. When we found out about the abuse, we shut this feature down. In the past, we have been aware of scraping as an industry issue, and have dealt with specific bad actors.

With respect to how we make decisions about privacy, at Facebook, we evaluate these questions through a cross-functional, cross-disciplinary effort overseen by the Chief Privacy Officer that involves participants from departments across the company. This process is a collaborative approach to privacy that seeks to promote strong privacy protections and sound decision making at every stage of the product development process. Our privacy program is responsible for reviewing product launches, major changes, and privacy-related bug fixes to products and features to ensure that privacy policies and procedures are consistently applied and that key privacy decisions are implemented for the product. This approach has several key benefits:

- First, it is designed to consider privacy early in the product development process. This allows us to consider the benefits that a feature is intended to have for people who use our services, how data will be used to deliver those benefits, and how we can build features from the ground up that include privacy protections to enable those benefits while protecting people's information and putting them in control.

- Second, while complying with our obligations is critically important, taking a cross-disciplinary approach to privacy encourages us to think about data protection as more than just a compliance exercise. Instead, we evaluate how to design privacy into the features that we build and consider this from the perspective of things like how we design interfaces that make data use intuitive, taking a consistent approach to privacy across our services, and building protections in how our software is engineered. Accordingly, while we scale our privacy review process depending on the complexity of a particular data use, reviews typically involve experts who evaluate proposed data practices from the perspective of multiple disciplines.

Further, as part of our consent agreement with the Federal Trade Commission, we submit a report to the FTC every two years. That report is based on assessments conducted by an

independent third party, which obtains evidence to evaluate the design and test the operating effectiveness of the privacy controls.

3. <u>Third-Party Applications</u>: Until 2014, Facebook's application program interface (API) allowed third-party applications to collect data not only from users of those apps, but also from the people in those users' friends network.

a. Why did Facebook wait so long to eliminate this function?

In 2007, there was industry-wide interest in enriching and expanding users' experiences on various platforms by allowing them to take their data (from a device or service) to third-party developers to receive new experiences. For example, around that time, Apple and Google respectively launched their iOS and Android platforms, which were quickly followed by platform technologies and APIs that allowed developers to develop applications for those two platforms and distribute them to users through a variety of channels. Similarly, in 2007, Facebook launched a set of platform technologies that allowed third parties to build applications that could run on and integrate with the Facebook service and that could be installed by Facebook users who chose to do so. In December 2009, Facebook launched new privacy controls that enabled users to control which of the types of information that they made available to their friends could be accessed by apps used by those friends.

As with all of these platforms, the permissions model that governed the information that third-party applications could access from the Platform evolved. For example, in April 2010, Facebook launched granular data permissions (GDP), which allowed users to examine a list of categories of information that an app sought permission to access before they authorized the app.

Throughout the relevant period and through today, Facebook's policies regarding third-party usage of its platform technologies have prohibited—and continue to prohibit—third-party app developers from selling or licensing user data obtained from Facebook or from sharing any user data obtained from Facebook with any ad network, data broker or other advertising or monetization-related service.

In November 2013, when Kogan launched the app, apps generally could be launched on the Platform without affirmative review or approval by Facebook. The app used the Facebook Login service, which allowed users to utilize their Facebook credentials to authenticate themselves to third-party services. Facebook Login and Facebook's Graph API also allowed the app to request permission from its users to bring their Facebook data (their own data and data shared with them by their friends) to the app, to obtain new experiences.

At that time, the Graph API V1 allowed app developers to request consent to access information from the installing user such as name, gender, birthdate, location (i.e., current city or hometown), photos and Page likes—and also (depending on, and in accordance with, each friend's own privacy settings) the same or similar categories of information the user's friends had shared with the installing user. Permitting users to share data made available to them by their friends had the upside of making the experience of app users more personalized and social. For example, a Facebook user might want to use a music app that allowed the user to (1) see what his or her friends were listening to and (2) give the app permission to access the user's friend list and

thereby know which of the user's friends were also using the app. Such access to information about an app user's friends required not only the consent of the app user, but also required that the friends whose data would be accessed have their own privacy settings set to permit such access by third-party apps. In other words, Kogan's app could have accessed a user's friends' information only for friends whose privacy settings permitted such sharing.

In April 2014, we announced that we would more tightly restrict our platform APIs to prevent abuse. At that time, we made clear that existing apps would have a year to transition—at which point they would be forced (1) to migrate to the more restricted API and (2) be subject to Facebook's new review and approval protocols. The vast majority of companies were required to make the changes by May 2015; a small number of companies (fewer than 100) were given a one-time extension of less than six months beyond May 2015 to come into compliance. (One company received an extension to January 2016.) In addition, in the context of our ongoing review of third-party apps, we discovered a very small number of companies (fewer than 10) that theoretically could have accessed limited friends' data as a result of API access that they received in the context of a beta test. We are not aware that any of this handful of companies used this access, and we have now revoked any technical capability they may have had to access any friends' data.

New apps that launched after April 30, 2014 were required to use our more restrictive platform APIs, which incorporated several key new elements, including:

- Institution of a review and approval process, called App Review (also called Login Review), for any app seeking to operate on the new platform that would request access to data beyond the user's own public profile, email address, and a list of friends of the user who had installed and authorized the same app;

- Generally preventing new apps on the new platform from accessing friends data without review; and

- Providing users with even more granular controls over their permissions as to what categories of their data an app operating on the new platform could access.

Our investigation is ongoing and as part of it we are taking a close look at applications that had access to friends data under Graph API V1 before we made technical changes to our platform to change this access.

The App Review process introduced in 2014 required developers who create an app that asks for more than certain basic user information to justify the data they are looking to collect and how they are going to use it. Facebook then reviewed whether the developer has a legitimate need for the data in light of how the app functions. Only if approved following such review can the app ask for a user's permission to get their data. Facebook has rejected more than half of the apps submitted for App Review between April 2014 and April 2018, including Kogan's second app. We are changing Login so that the only data that an app can request without app review will include name, profile photo, and email address.

b. What did Facebook believe was the benefit of this arrangement to Facebook's users?

See Response to Question 3(a).

c. How many third-party entities were authorized to collect the date of Facebook users' friends? Can Facebook identify each of these entities?

We are in the process of investigating every app that had access to a large amount of information before we changed our Platform in 2014. The investigation process is in full swing, and it has two phases. First, a comprehensive review to identify every app that had access to this amount of Facebook data and to focus on apps that present reason for deeper investigation. And second, where we have concerns, we will conduct interviews, make requests for information (RFI)—which ask a series of detailed questions about the app and the data it has access to—and perform audits using expert firms that may include on-site inspections. We have large teams of internal and external experts working hard to investigate these apps as quickly as possible. As of early June 2018, thousands of apps have been investigated and around 200 apps have been suspended—pending a thorough investigation into whether they did in fact misuse any data. Where we find evidence that these or other apps did misuse data, we will ban them and let people know.

These apps relate to a handful of developers: Kogan, AIQ, Cube You, the Cambridge Psychometrics Center, and myPersonality, with many of the suspended apps being affiliated with the same entity. Many of these suspensions include apps that appear to be "test" apps that were never released to the public, and therefore would not have acquired significant user data, although our investigation into these apps is ongoing.

Additionally, we have suspended an additional 14 apps, which were installed by around one thousand people. They were all created after 2014, after we made changes to more tightly restrict our platform APIs to prevent abuse. However, these apps appear to be linked to AIQ, which was affiliated with Cambridge Analytica. So, we have suspended them while we investigate further. Any app that refuses to take part in or fails our audit will be banned.

d. Does Facebook know what happened to that data and whether it was shared further?

See Response to Question 3(c).

e. Does Facebook have an estimate of how many users were exposed in this way?

See Response to Question 3(c).

f. Is it possible that every Facebook user's personal data has been shared in an unauthorized way by third-party applications?

See Response to Question 3(c).

g. What harms could and should users expect to experience?

See Response to Question 3(a).

h. How is Facebook prepared to remedy those harms?

See Response to Question 3(a).

i. Will Facebook notify users that their data has been inappropriately exposed to other third-party entities?

See Response to Question 3(c).

j. How does Facebook audit third-party applications to ensure that they are who they say they are?

We use a variety of tools to enforce Facebook policies against violating parties, including developers. We review tens of thousands of apps per year and regularly disapprove noncompliant apps as part of our proactive review process. We also use tools like cease-and-desist letters, account suspensions, letter agreements, and civil litigation. For example, since 2006, Facebook has sent over 1,150 cease-and-desist letters to over 1,600 targets. In 2017, we took action against about 370,000 apps, ranging from imposing certain restrictions to removal of the app from the platform. Moreover, we have required parties who have procured our data without authorization to delete that data. We have invested significant resources in these efforts. Facebook is presently investigating apps that had access to large amounts of information before we changed our platform policies in 2014 to significantly reduce the data apps could access. As of early June 2018, around 200 apps (from a handful of developers: Kogan, AIQ, Cube You, the Cambridge Psychometrics Center, myPersonality, and AIQ) have been suspended—pending a thorough investigation into whether they did in fact misuse any data.

k. Under Facebook's current policies and practices, what information and data can apps acquire about their users? Their users' friends?

See Response to Question 3(a).

4. <u>Sharing Data with Third Parties</u>: When Facebook shares data with third parties subject to a contract or a terms of service agreement, how does it verify and ensure those terms are followed?

a. Does Facebook evaluate the third parties' data security policies, data retention policies, or intended uses for the data when it shares data?

See Response to Question 3(a).

Recently, we announced a number of additional steps we're taking to address concerns raised by Kogan's app.

- **Review our platform.** We are investigating all apps that had access to large amounts of data before the platform changes we announced in 2014, and we will audit any app where we identify suspicious activity. If we identify misuses of data, we'll take immediate action, including banning the app from our platform and pursuing legal action if appropriate.

- **Tell people about data misuse.** We will tell people about apps that have misused their data.

- **Turn off access for unused apps.** If someone has not used an app within the last three months, we will turn off the app's access to their data.

- **Restrict Facebook Login data.** We are changing Login, so that the only data that an app can request without app review will include name, profile photo, and email address. Requesting any other data will require approval from Facebook. We will also no longer allow apps to ask for access to information like religious or political views, relationship status and details, custom friends lists, education and work history, fitness activity, book reading and music listening activity, news reading, video watch activity, and games activity. We will encourage people to manage the apps they use. We already show people what apps their accounts are connected to and allow them to control what data they've permitted those apps to use. But we're making it easier for people to see what apps they use and the information they have shared with those apps.

- **Reward people who find vulnerabilities.** We launched the Data Abuse Bounty program so that people can report to us any misuses of data by app developers.

- **Update our policies.** We have updated our terms and Data Policy to explain in more detail how we use data and how data is shared with app developers.

b. If so, how often are third-party data policies reevaluated and reapproved?

See Response to Questions 3(a) and 4(a).

c. In addition to researchers, what other types of third parties are allowed access to Facebook data?

In our Data Policy, we explain that we may use the information we have to conduct and support research in areas that may include general social welfare, technological advancement, public interest, health and well-being. Researchers are subject to strict restrictions regarding data access and use as part of these collaborations.

We are investigating all apps that, like Aleksandr Kogan's, had access to large amounts of information before we changed our platform in 2014 to reduce data access. The investigation process is in full swing, and it has two phases. First, a comprehensive review to identify every app that had access to this amount of Facebook data. And second, where we have concerns, we will conduct interviews, make requests for information (RFI)—which ask a series of detailed

questions about the app and the data it has access to—and perform audits that may include on-site inspections. We have large teams of internal and external experts working hard to investigate these apps as quickly as possible. As of early June 2018, thousands of apps have been investigated and around 200 (from a handful of developers: GSR, Cube You, the Cambridge Psychometrics Center, myPersonality, and AIQ) have been suspended—pending a thorough investigation into whether they did in fact misuse any data. Where we find evidence that these or other apps did misuse data, we will ban them and notify people whose data was shared with these apps.

5. **Facebook and ICE: In response to a recent article about Immigration and Customs Enforcement (ICE)'s use of your platform, Facebook said, "Facebook does not provide ICE or any other law enforcement agency with any special data access to assist with the enforcement of immigration law. We have strict processes in place to handle these government requests. Every request we receive is checked for legal sufficiency. We require officials to provide a detailed description of the legal and factual basis for their request, and we push back when we find legal deficiencies or overly broad or vague demands for information."**

   a. **Can you expand on Facebook's process for responding to this type of requests? How does Facebook determine what is a legally sufficient request?**

   b. **How does Facebook "push back" when it receives a legally deficient, "overly broad" or "vague" demand for information?**

   c. **What kind of information does Facebook provide to ICE once a request has been deemed legally sufficient? Is this information different in any way from what Facebook provides to other law enforcement agencies?**

   d. **How many requests has ICE made of Facebook in the past year? How many were determined to be legitimate?**

We disclose account records solely in accordance with our terms of service and applicable law, including the federal Stored Communications Act (SCA), 18 U.S.C. Sections 2701-2712. If requests appear to be legally deficient, overly broad, or vague, our Law Enforcement Response team will reject the requests outright or contact the law enforcement agency that issued the legal process for more information and to work to narrow the scope of the legal process so that it is limited to the users and data relevant to the criminal investigation.

The information that ICE or any other law enforcement authority in the US may request from a provider depends on the type of legal process authorizing the disclosure. Under US law, a valid subpoena issued in connection with an official criminal investigation is required to compel the disclosure of basic subscriber records (defined in 18 U.S.C. Section 2703(c)(2)), which may include: name, length of service, credit card information, email address(es), and a recent login/logout IP address(es), if available. A court order issued under 18 U.S.C. Section 2703(d) is required to compel the disclosure of certain records or other information pertaining to the account, not including contents of communications, which may include message headers and IP addresses, in addition to the basic subscriber records identified above. A search warrant issued

under the procedures described in the Federal Rules of Criminal Procedure or equivalent state warrant procedures upon a showing of probable cause is required to compel the disclosure of the stored contents of any account, which may include messages, photos, videos, timeline posts, and location information.

Our policy is to notify people who use our service of requests for their information prior to disclosure unless we are prohibited by law from doing so or in exceptional circumstances, such as child exploitation cases, emergencies, or when notice would be counterproductive. We will also provide delayed notice upon expiration of a specific non-disclosure period in a court order and where we have a good faith belief that exceptional circumstances no longer exist and we are not otherwise prohibited by law from doing so. Law enforcement officials who believe that notification would jeopardize an investigation are directed to obtain an appropriate court order or other appropriate process establishing that notice is prohibited.

In 2017, we received about 65,000 requests from US law enforcement authorities in connection with criminal investigations and produced some data in response to 85% of those requests. For more information about our responses to government requests broken down by country, please see our Transparency Report (https://transparency.facebook.com/).

The Honorable Paul Tonko

1. Facebook trains many of its advertising customers on how to access its users' information. David of Saratoga Springs, New York expressed concern that Facebook may have provided training to Russian agents. Is it possible that Facebook has directly provided training to these bad actors?

The vast majority of our over 5 million advertisers use our self-service tools. This allows individuals or businesses to create a Facebook Page, attach a credit card or some other payment method, and run ads promoting their posts.

Further, while we provide advertisers with reports about the kinds of people seeing their ads and how their ads are performing, we don't share information that personally identifies people (information such as name or that by itself can be used to contact or identifies a person) unless we have permission from people. For example, we provide statistical demographic information to advertisers (e.g., that an ad was seen by 2,436 women between the ages of 25 and 34 in Maryland) to help them better understand their audience.

We give people a number of controls over the data we use to show them ads. These controls apply to our use of data to show people ads; they do not apply to the collection of data, because the same core data sets are used to ensure the safety and security of our platform and to provide our core service to our users. As noted above, people can see and control the advertising "interests" and "behaviors" we have associated with their accounts to show them ads. They can choose not to see ads from a particular advertiser or not to see ads based on their use of third-party websites and apps. They also can choose not to see ads off Facebook that are based on the interests we derive from their activities on Facebook.

In some situations, Facebook employees work directly with our larger advertisers. In the case of the Russian ads, none of those we found involved in-person relationships.

2. Another New Yorker, Stephanie asked how can we be sure that Cambridge Analytica or its parent company or GSR does not continue to improperly retain our data? Do foreign countries, companies, businesses still have our data? Or do they have access to it in other ways?

In March 2018, we learned from news reports that contrary to the certifications given, not all of the Kogan data may have been deleted by Cambridge Analytica. We have no direct evidence of this and no way to confirm this directly without accessing Cambridge Analytica's systems and conducting a forensic audit. We have held off on audits of Cambridge Analytica and other parties that are being investigated by the UK Information Commissioner's Office at its request. Our investigation is ongoing.

3. Sean of Albany New York asked, "Is this an isolated incident? How many other companies like Cambridge Analytica are out there with this kind of data?"

Facebook is in the process of investigating all the apps that had access to large amounts of information, such as extensive friends data (if those friends' privacy data settings allowed sharing), before we changed our platform policies in 2014—significantly reducing the data apps

could access. Where we have concerns about individual apps, we are investigating them—and any app that either refuses or fails an audit will be banned from Facebook. As of early June 2018, thousands of apps have been investigated and around 200 have been suspended—pending a thorough investigation into whether they did in fact misuse any data.

These apps relate to a handful of developers: Kogan, AIQ, Cube You, the Cambridge Psychometrics Center, and myPersonality, with many of the suspended apps being affiliated with the same entity. Many of these apps also appear to be "test" apps that were never released to the public, and therefore would not have acquired significant user data, although our investigation into these apps is ongoing.

Additionally, we have suspended an additional 14 apps, which were installed by around one thousand people. They were all created after 2014, after we changed our platform to reduce data access. However, these apps appear to be linked to AIQ, which was affiliated with Cambridge Analytica. So, we have suspended them while we investigate further. Any app that refuses to take part in or fails our audit will be banned.

4. Jeremy, of Waterford New York asked, "What, specifically, is Facebook doing to ensure that a data breach of this scale will not happen again in the future, and how will Facebook make amends to the 87 million affected users?

In April 2014, we announced that we would more tightly restrict our platform APIs to prevent abuse. At that time, we made clear that existing apps would have a year to transition—at which point they would be forced (1) to migrate to the more restricted API and (2) be subject to Facebook's new review and approval protocols. The vast majority of companies were required to make the changes by May 2015; a small number of companies (fewer than 100) were given a one-time extension of less than six months beyond May 2015 to come into compliance. (One company received an extension to January 2016.) In addition, in the context of our ongoing review of third-party apps, we discovered a very small number of companies (fewer than 10) that theoretically could have accessed limited friends' data as a result of API access that they received in the context of a beta test. We are not aware that any of this handful of companies used this access, and we have now revoked any technical capability they may have had to access any friends' data.

New apps that launched after April 30, 2014 were required to use our more restrictive platform APIs. We required apps seeking additional categories of data to undergo proactive review by our internal teams. We rejected more than half of the apps seeking these permissions, including the second version of Kogan's app.

We review apps to ensure that the requested permissions clearly improve the user experience and that the data obtained is tied to an experience within the app. We conduct a variety of manual and automated checks of applications on the platform for Policy compliance, as well as random sampling. When we find evidence of or receive allegations of violations, we investigate and, where appropriate, employ a number of measures, including restricting applications from our platform, preventing developers from building on our platform in the future, and taking legal action where appropriate.

Recently, we announced a number of additional steps we're taking to address concerns raised by Kogan's app:

- **Review our platform.** We will investigate all apps that had access to large amounts of data before the platform changes we announced in 2014, and we will audit any app where we identify suspicious activity. If we identify misuses of data, we'll take immediate action, including banning the app from our platform and pursuing legal action if appropriate.

- **Tell people about data misuse.** We will tell people about apps that have misused their data.

- **Turn off access for unused apps.** If someone has not used an app within the last three months, we will turn off the app's access to their data.

- **Restrict Facebook Login data.** We are changing Login, so that the only data that an app can request without app review will include name, profile photo, and email address. Requesting any other data will require approval from Facebook. We will also no longer allow apps to ask for access to information like religious or political views, relationship status and details, custom friends lists, education and work history, fitness activity, book reading and music listening activity, news reading, video watch activity, and games activity. We will encourage people to manage the apps they use. We already show people what apps their accounts are connected to and allow them to control what data they've permitted those apps to use. But we're making it easier for people to see what apps they use and the information they have shared with those apps.

- **Reward people who find vulnerabilities.** We launched the Data Abuse Bounty program so that people can report to us any misuses of data by app developers.

- **Update our policies.** We have updated our terms and Data Policy to explain how we use data and how data is shared with app developers.

We are investing so much in security that our costs will increase significantly. But we want to be clear about what our priority is: protecting our community is more important than maximizing our profits.

As our CEO Mark Zuckerberg has said, when you are building something unprecedented like Facebook, there are going to be mistakes. What people should hold us accountable for is learning from the mistakes and continually doing better—and, at the end of the day, making sure that we're building things that people like and that make their lives better.

The Honorable Kurt Schrader

1. In 2014 Facebook announced it would introduce Anonymous Login to allow users to log into apps without sharing personal information. Why hasn't Facebook rolled this feature out?

We rolled out Anonymous Login in beta to a number of developers. Although there was significant interest at launch, ultimately few developers wanted to use it. We believe this was because Anonymous Login did not provide features that enabled app developers to communicate directly with their users. Because of light adoption, we started phasing out Anonymous Login in the second half of 2015. We have since launched another product, Account Kit, that does not require a Facebook account and gives people the choice to log into new apps with just their phone number or email address.

The Honorable Joseph Kennedy

1. This hearing, and the ongoing conversations about privacy on the Internet, have highlighted the stunning amount of personal information that social media websites scavenge, store, and sell with little regard for establishing the safeguards such information deserves. While platforms such as Facebook certainly can work for good, like helping loved ones connect after a disaster, the 2016 election demonstrated its ability to manipulate personal data, spread misinformation and interfere in democratic processes.

Facebook collects several types of data, from information users share about themselves or other users to online activities and behavior, information purchased from other data brokers, and information that the platform's algorithms and A1 allow it to infer. Some of this data the public willingly offers to Facebook, such as profile pictures, names, and email addresses and some of that information users can designate as private or only available to friends. However, Facebook also collects data about which users are unaware, like users' physical locations, where they shop, websites they frequent, and information it scrapes off of users browsing history, even after they have logged out of Facebook. Facebook then manipulates both types of data into predictive models about how we behave, what we believe, and the values we hold dear.

Mr. Zuckerberg, you have said that Facebook users own their data and have complete control over it. However, users aren't paid for the commercial use and exploitation of their data, don't know the extent of its existence and retention, and typically provide only superficial consent for its collection. When you say that Facebook users own their data and have complete control over it, are you referring to all data that Facebook and its affiliates maintain, including all four types mentioned above? That includes all data used to target advertisements and influence behavior? Is there any information about themselves that users cannot access, control, or correct in the event it is erroneous? Do they "own" the information generated by your algorithms or artificial intelligence programs? If so, how can they get it, protect it, or erase it?

Additionally, are users able to restrict the use of the data that Facebook collects, data not intended to be shared publicly, to target them for advertisements? Are users able to see how data about them has been used for ad targeting, e.g. "Why am I seeing this ad?"

We believe that it's important to communicate with people about the information that we collect and how people can control it. That is why we work hard to provide this information to people in a variety of ways: in our Data Policy, and in Privacy Basics, which provides walkthroughs of the most common privacy questions we receive. Depending on which Services a person uses, we collect different kinds of information from or about them. This is described in our Data Policy:

- **Things users and others do and provide.** Information and content users provide. We collect the content, communications and other information users provide when they use our Products, including when they sign up for an account, create or share content, and message or communicate with others. This can include information in or about the content they provide (like metadata), such as the location of a photo or the date a file was created. It can also include what users see through features we provide, such as our camera, so we can do things like suggest masks and filters that they might like, or give users tips on using camera formats. Our systems automatically process content and communications users provide to analyze context and what's in them for the purposes described below. People can learn more about how they can control who can see the things they share here: https://www.facebook.com/help/1297502253597210?ref=dp.

    - Data with special protections: Users can choose to provide information in their Facebook profile fields or Life Events about their religious views, political views, who they are "interested in," or their health. This and other information (such as racial or ethnic origin, philosophical beliefs, or trade union membership) could be subject to special protections under the laws of their country.

- **Networks and connections**. We collect information about the people, Pages, accounts, hashtags, and groups users are connected to and how they interact with them across our Products, such as people a user communicates with the most or groups users are part of. We also collect contact information if they choose to upload, sync, or import it from a device (such as an address book or call log or SMS log history), which we use for things like helping them and others find people they may know and for the other purposes listed in our Data Policy.

- **People's usage**. We collect information about how people use our Products, such as the types of content they view or engage with; the features they use; the actions they take; the people or accounts they interact with; and the time, frequency, and duration of their activities. For example, we log when they're using and have last used our Products, and what posts, videos, and other content they view on our Products. We also collect information about how they use features like our camera.

- **Information about transactions made on our Products**. If people use our Products for purchases or other financial transactions (such as when users make a purchase in a game or make a donation), we collect information about the purchase or transaction. This includes payment information, such as their credit or debit card number and other card information; other account and authentication information; and billing, shipping, and contact details.

- **Things others do and information they provide about users**. We also receive and analyze content, communications, and information that other people provide when they use our Products. This can include information about them, such as when others share or comment on a photo of a user, send a message to them, or upload, sync or import their contact information.

- **Device Information.** As described below, we collect information from and about the computers, phones, connected TVs and other web-connected devices they use that integrate with our Products, and we combine this information across different devices they use. For example, we use information collected about their use of our Products on their phone to better personalize the content (including ads) or features they see when they use our Products on another device, such as their laptop or tablet, or to measure whether they took an action in response to an ad we showed them on their phone on a different device.
    - Information we obtain from these devices includes:
        - Device attributes: information such as the operating system, hardware and software versions, battery level, signal strength, available storage space, browser type, app and file names and types, and plugins.
        - Device operations: information about operations and behaviors performed on the device, such as whether a window is foregrounded or backgrounded, or mouse movements (which can help distinguish humans from bots).
        - Identifiers: unique identifiers, device IDs, and other identifiers, such as from games, apps or accounts people use, and Family Device IDs (or other identifiers unique to Facebook Company Products associated with the same device or account).
        - Device signals: Bluetooth signals, and information about nearby Wi-Fi access points, beacons, and cell towers.
        - Data from device settings: information users allow us to receive through device settings people turn on, such as access to their GPS location, camera, or photos.
        - Network and connections: information such as the name of users' mobile operator or ISP, language, time zone, mobile phone number, IP address, connection speed and, in some cases, information about other devices that are nearby or on users' network, so we can do things like help people stream a video.
        - Cookie data: data from cookies stored on a user's device, including cookie IDs and settings. Learn more about how we use cookies in the Facebook Cookies Policy (https://www.facebook.com/policies/cookies/) and Instagram Cookies Policy (https://www.instagram.com/legal/cookies/).
- **Information from partners**. Advertisers, app developers, and publishers can send us information through Facebook Business Tools they use, including our social plug-ins (such as the Like button), Facebook Login, our APIs and SDKs, or the Facebook pixel. These partners provide information about users' activities off Facebook—including information about a user's device, websites users visit, purchases users make, the ads

they see, and how they use their services—whether or not they have a Facebook account or are logged into Facebook. For example, a game developer could use our API to tell us what games users play, or a business could tell us about a purchase a user made in its store. We also receive information about a user's online and offline actions and purchases from third-party data providers who have the rights to provide us with their information. Partners receive user data when users visit or use their services or through third parties they work with. We require each of these partners to have lawful rights to collect, use and share user data before providing any data to us.

We've heard loud and clear that privacy settings and other important tools are too hard to find and that we must do more to keep people informed. So, we're taking additional steps to put people more in control of their privacy. For instance, we redesigned our entire settings menu on mobile devices from top to bottom to make things easier to find. We also created a new Privacy Shortcuts in a menu where users can control their data in just a few taps, with clearer explanations of how our controls work. The experience is now clearer, more visual, and easy-to-find. Furthermore, we also updated our terms of service that include our commitments to everyone using Facebook. We explain the services we offer in language that's easier to read.

Any person can see each of the specific interests we maintain about them for advertising by visiting Ads Preferences, which lets people see what interests we use to choose ads for them—and to edit or delete these interests. They can choose not to see ads from a particular advertiser or not to see ads based on their use of third-party websites and apps. They also can choose not to see ads off Facebook that are based on the interests we derive from their activities on Facebook.

People own what they share on Facebook, and they can manage things like who sees their posts and the information they choose to include on their profile. Facebook does not sell people's information to anyone, and we never will. We also impose strict restrictions on how our partners can use and disclose the data we provide.

Our Download Your Information or "DYI" tool is Facebook's data portability tool and was launched many years ago to let people access and download many types of information that we maintain about them. The data in DYI and in our Ad Preferences tool contain each of the interest categories that are used to show people ads, along with information about the advertisers that are running ads based on their use of an advertiser's website or app. People also can choose not to see ads from those advertisers. We recently announced expansions to Download Your Information, which, among other things, will make it easier for people to see their data, delete it, and easily download and export it. More information is available at https://newsroom.fb.com/news/2018/04/new-privacy-protections/.

We have also introduced Access Your Information, a new tool that builds on the functionality we provide in Download Your Information. This feature provides a new way for people to access and manage their information. Users can go here to delete anything from their timeline or profile that they no longer want on Facebook. They can also see their ad interests, as well as information about ads they've clicked on and advertisers who have provided us with information about them that influence the ads they see. From here, they can go to their ad settings to manage how this data is used to show them ads.

Responding to feedback that we should do more to provide information about websites and apps that send us information when people use them, we also announced plans to build Clear History. This new feature will enable users to see the websites and apps that send us information when they use them, clear this information from their account, and turn off Facebook's ability to store it associated with their account going forward.

Further, when a person visiting a website featuring Facebook's tools is not a registered Facebook user, Facebook does not have information identifying that individual, and it does not create profiles for this individual.

2. At its core, Facebook serves as a platform that allows users to connect to others and with various entities (businesses, campaigns, non-profits) that may advertise, advocate, or otherwise attempt to influence the behavior of users. While Facebook has indicated that the company will take various steps to prevent prohibited use of their platform and increase user protections and consent, those reforms do nothing to address the structural issue at hand. As long as the platform can be used for influence, entities will use it to influence - be they companies, foreign intelligence agencies, or other abusers. How should we think about this risk and what, if anything, should Facebook do to address it? Are reforms necessary to protect our democracy?

Protecting a global community of more than 2 billion involves a wide range of teams and functions, and our expectation is that those teams will grow across the board. For example, we have dedicated information security and related engineering teams.

Protecting the security of information on Facebook is at the core of how we operate. Security is built into every Facebook product, and we have dedicated teams focused on each aspect of data security. From encryption protocols for data privacy to machine learning for threat detection, Facebook's network is protected by a combination of advanced automated systems and teams with expertise across a wide range of security fields. Our security protections are regularly evaluated and tested by our own internal security experts and independent third parties. For the past seven years, we have also run an open bug bounty program that encourages researchers from around the world to find and responsibly submit security issues to us so that we can fix them quickly and better protect the people who use our service.

We anticipate continuing to grow these teams by hiring a range of experts, including people with specific types of threat intelligence expertise.

This will never be a solved problem because we're up against determined, creative and well-funded adversaries. But we are making steady progress. Here is a list of the 10 most important changes we have made:

- **Ads transparency.** Advertising should be transparent: users should be able to see all the ads an advertiser is currently running on Facebook, Instagram, and Messenger. And for ads with political content, we've created an archive that will hold ads with political content for seven years—including information about ad impressions and spend, as well as demographic data such as age, gender and location. People in

Canada and Ireland can already see all the ads that a Page is running on Facebook—and we've launched this globally.

- **Verification and labeling.** Every advertiser will now need to confirm their ID and location before being able to run any ads with political content in the US. All ads with political content will also clearly state who paid for them.

- **Updating targeting.** We want ads on Facebook to be safe and civil. We thoroughly review the targeting criteria advertisers can use to ensure they are consistent with our principles. As a result, we removed nearly one-third of the targeting segments used by the IRA. We continue to allow some criteria that people may find controversial. But we do see businesses marketing things like historical books, documentaries or television shows using them in legitimate ways.

- **Better technology.** Over the past year, we've gotten increasingly better at finding and disabling fake accounts. We now block millions of fake accounts each day as people try to create them—and before they've done any harm. This is thanks to improvements in machine learning and artificial intelligence, which can proactively identify suspicious behavior at a scale that was not possible before—without needing to look at the content itself.

- **Action to tackle fake news.** We are working hard to stop the spread of false news. We work with third-party fact-checking organizations to limit the spread of articles rated false. To reduce the spread of false news, we remove fake accounts and disrupt economic incentives for traffickers of misinformation. We also use various signals, including feedback from our community, to identify potential false news. In countries where we have partnerships with independent third-party fact-checkers, stories rated as false by those fact-checkers are shown lower in News Feed. If Pages or domains repeatedly create or share misinformation, we significantly reduce their distribution and remove their advertising rights. We also want to empower people to decide for themselves what to read, trust, and share. We promote news literacy and work to inform people with more context. For example, if third-party fact-checkers write articles about a news story, we show them immediately below the story in the Related Articles unit. We also notify people and Page Admins if they try to share a story, or have shared one in the past, that's been determined to be false. In addition to our own efforts, we're learning from academics, scaling our partnerships with third-party fact-checkers and talking to other organizations about how we can work together.

- **Significant investments in security.** We're doubling the number of people working on safety and security from 10,000 last year to over 20,000 this year. We expect these investments to impact our profitability. But the safety of people using Facebook needs to come before profit.

- **Industry collaboration.** Recently, we joined 34 global tech and security companies in signing a TechAccord pact to help improve security for everyone.

- **Information sharing and reporting channels.** In the 2017 German elections, we worked closely with the authorities there, including the Federal Office for Information Security (BSI). This gave them a dedicated reporting channel for security issues related to the federal elections.

- **Tracking 40+ elections.** In recent months, we've started to deploy new tools and teams to proactively identify threats in the run-up to specific elections. We first tested this effort during the Alabama Senate election, and plan to continue these efforts for elections around the globe, including the US midterms. Last year we used public service announcements to help inform people about fake news in 21 separate countries, including in advance of French, Kenyan and German elections.

- **Action against the Russia-based IRA.** In April, we removed 70 Facebook and 65 Instagram accounts—as well as 138 Facebook Pages—controlled by the IRA primarily targeted either at people living in Russia or Russian-speakers around the world including from neighboring countries like Azerbaijan, Uzbekistan, and Ukraine. The IRA has repeatedly used complex networks of inauthentic accounts to deceive and manipulate people in the US, Europe, and Russia—and we don't want them on Facebook anywhere in the world.

We are taking steps to enhance trust in the authenticity of activity on our platform, including increasing ads transparency, implementing a more robust ads review process, imposing tighter content restrictions, and exploring how to add additional authenticity safeguards.

The Honorable Tony Cárdenas

1. Diversity:

a. How many Hispanic employees work at Facebook?

i What percentage is that of all Facebook employees?

ii How many work in technical positions?

iii How many work in managerial positions?

iv How many work in executive positions?

b. How many Hispanic employees work at Facebook in the United States?

i What percentage is that of all U.S. Facebook employees?

ii How many work in technical positions?

iii How many work in managerial positions?

iv How many work in executive positions?

c. How many Hispanic employees work at Facebook headquarters in Menlo Park?

i What percentage is that of all Facebook HQ employees?

ii How many work in technical positions?

iii How many work in managerial positions?

iv How many work in executive positions?

d. Do you believe that a company whose staff does not reflect the diversity of the United States is able to design Artificial Intelligence systems that are free of ethnic bias?

With a global community of over two billion people on Facebook, greater diversity and inclusivity are critical to achieving our mission. Studies have shown that cognitive diversity on teams that are working on hard problems produces better results. Diversity helps us build better products, make better decisions and better serve our community. In order to achieve that, we have developed programming to attract and retain more people from traditionally underrepresented groups which include women, people of color, veterans, and people with disabilities.

We are not where we would like to be, but we are encouraged that representation for people from underrepresented groups at Facebook has increased. We've grown Black and

Hispanic representation by 1 percent each (2 percent combined) between our first report in 2014 and our most recent report in 2017 (note that ethnicity data is for US employees):

- Black Representation: from 2 percent to 3 percent
- Hispanic Representation: from 4 percent to 5 percent
- Black Non-Tech: from 2 percent to 6 percent
- Hispanic Non-Tech: from 6 percent to 8 percent
- Black Leadership: from 2 percent to 3 percent
- Hispanic Leadership: from 4 percent to 3 percent
- Black and Hispanic Tech have stayed at 1 percent and 3 percent

As of August 2017, the number of women globally increased from 33 percent to 35 percent:

- Women in Tech: from 17 percent to 19 percent
- Women in Non-Tech: from 47 percent to 55 percent
- Women in Leadership: from 23 percent to 28 percent
- Women made up 27 percent of all new graduate hires in engineering and 21 percent of all new technical hires at Facebook.

We seek to promote diversity in a variety of ways, and we want to highlight three programs in particular. First, we have adopted our Diverse Slate Approach (DSA) to interviewing job candidates. The more people that hirers interview who don't look or think like them, the more likely they are to hire someone from a diverse background. To hardwire this behavior at Facebook, we introduced our DSA in 2015 and have since rolled it out globally. DSA sets the expectation that hiring managers will consider candidates from underrepresented backgrounds when interviewing for an open position.

Second, we are working to reduce unconscious bias. Our publicly available Managing Unconscious Bias class encourages our people to challenge and correct bias as soon as they see it—in others, and in themselves. We've also doubled down by adding two additional internal programs: Managing Inclusion, which trains managers to understand the issues that affect marginalized communities, and Be The Ally, which gives everyone the common language, tools, and space to practice supporting others.

Third, we have created Facebook University. We want to increase access and opportunity for students with an interest in software engineering, business, and analytics. Facebook University (FBU) gives underrepresented students extra training and mentorship earlier in their college education. We started FBU in 2013 with 30 students and expect to have 280 in 2018.

More than 500 students have graduated from this program, with many returning to Facebook for internships and full-time jobs.

Finally, we have many partnerships to move the numbers nationally such as Black Girls Code, All Star Code, Hack the Hood, The Hidden Genius Project, Level Playing Field Institute, Yes We Code, Streetcode Academy, Dev Color, Dev Bootcamp and Techbridge. And, we now recruit at 300 Universities—including historically black colleges and universities (HBCUs) like Spelman, Morehouse, Howard, NCA&T, and Morgan State (EIR) and the HBCU Faculty Summit.

We're committed to building a more diverse, inclusive Facebook. Much like our approach to launching new products on our platform, we are willing to experiment and listen to feedback.

Regarding AI, we are focused on both the technical and the ethical aspects of artificial intelligence. We believe these two should go hand-in-hand together in order to fulfill our commitment to being fair, transparent and accountable in our development and use of AI. Facebook has AI teams working on developing the philosophical, as well as technical, foundations for this work. Facebook is also one of the co-founders and members of the Partnership on AI (PAI), a collaborative and multi-stakeholder organization established to study and formulate best practices on AI technologies, to advance the public's understanding of AI, and to serve as an open platform for discussion and engagement about AI and its influences on people and society. The thematic pillars that structure the work we're doing in the scope of the PAI—safety, fairness, transparency and accountability—are the principles that we believe industry should follow and promote when building and deploying AI systems. The PAI's Fair, Transparent and Accountable AI Working Group is also working alongside industry, academia, and civil society to develop best practices around the development and fielding of fair, explainable, and accountable AI systems.

2. U.S. Immigration and Customs Enforcement (ICE): In response to a recent article about Immigration and Customs Enforcement (ICE)'s use of your platform, Facebook said, "Facebook does not provide ICE or any other law enforcement agency with any special data access to assist with the enforcement of immigration law. We have strict processes in place to handle these government requests. Every request we receive is checked for legal sufficiency. We require officials to provide a detailed description of the legal and factual basis for their request, and we push back when we find legal deficiencies or overly broad or vague demands for information."

a. Can you expand on Facebook's process for responding to this type of requests? How does Facebook determine what is a legally sufficient request?

We disclose account records solely in accordance with our terms of service and applicable law, including the federal Stored Communications Act (SCA), 18 U.S.C. Sections 2701-2712. The information that ICE or any other law enforcement authority in the US may request from a provider depends on the type of legal process authorizing the disclosure. Under US law, a valid subpoena issued in connection with an official criminal investigation is required

to compel the disclosure of basic subscriber records (defined in 18 U.S.C. Section 2703(c)(2)), which may include: name, length of service, credit card information, email address(es), and a recent login/logout IP address(es), if available. A court order issued under 18 U.S.C. Section 2703(d) is required to compel the disclosure of certain records or other information pertaining to the account, not including contents of communications, which may include message headers and IP addresses, in addition to the basic subscriber records identified above. A search warrant issued under the procedures described in the Federal Rules of Criminal Procedure or equivalent state warrant procedures upon a showing of probable cause is required to compel the disclosure of the stored contents of any account, which may include messages, photos, videos, timeline posts, and location information.

b. How many requests has ICE made of Facebook in the past year? How many were determined to be legitimate?

In 2017, we received about 65,000 requests from US law enforcement in connection with criminal investigations and produced some data in response to 85% of those requests. For more information about our responses to government requests broken down by country, please see our Transparency Report (https://transparency.facebook.com/).

c. Do you require a court order before you provide information to ICE?

See Response to Question 2(a).

d. What information does Facebook provide in cases where requests are determined to be legally sufficient?

See Response to Question 2(a).

e. Does Facebook notify users of the possibility that their information may be shared with ICE? If so, when?

Our policy is to notify people who use our service of requests for their information prior to disclosure unless we are prohibited by law from doing so or in exceptional circumstances, such as child exploitation cases, emergencies or when notice would be counterproductive. We will also provide delayed notice upon expiration of a specific non-disclosure period in a court order and where we have a good faith belief that exceptional circumstances no longer exist and we are not otherwise prohibited by law from doing so. Law enforcement officials who believe that notification would jeopardize an investigation should obtain an appropriate court order or other appropriate process establishing that notice is prohibited. If the data request draws attention to an ongoing violation of our terms of use, we will take action to prevent further abuse, including actions that may notify the user that we are aware of their misconduct.

f. How is the procedure for sharing data different if ICE produces a warrant?

See Response to Question 2(a).

g. How is the above-described procedure similar or different if ICE requests information from WhatsApp?

WhatsApp discloses account records solely in accordance with its terms of service and applicable law. For more information, please go to: https://faq.whatsapp.com/en/general/26000050.

h. How is the above-described procedure similar or different if ICE requests information from Instagram?

Instagram discloses account records solely in accordance its terms of service and applicable law, including the federal Stored Communications Act (SCA), 18 U.S.C. Sections 2701-2712. For more information, please go to: https://help.instagram.com/494561080557017.

3. Platform Responsibility: As you said multiple times during the hearing, in your view Facebook has a broader responsibility to make sure its tools are used for good.

a. Do you believe copyright infringement constitutes a good use of the Facebook platform?

b. Do you believe it is Facebook's responsibility to prevent copyright infringement on the platform?

We take intellectual property rights seriously at Facebook and work closely with the motion picture industries and other rights holders worldwide to help them protect their copyrights and other IP. Our measures target potential piracy across our products, including Facebook Live, and continue to be enhanced and expanded. These include a global notice-and-takedown program, a comprehensive repeat infringer policy, integration with the content recognition service Audible Magic, and our proprietary video- and audio-matching technology called Rights Manager. More information about these measures can be found in our Intellectual Property Help Center, Transparency Report, and Rights Manager website.

4. The Guardian:

a. Why did Facebook threaten to sue the newspaper *The Guardian* to stop *The Guardian* from publishing a story about Cambridge Analytica?

Facebook did not threaten to sue *The Guardian*. We sent *The Guardian* a letter to correct some facts in the article they sought to publish. Facebook supports vocal, independent journalism.

b. Why did Facebook wait until after *The Guardian* published the story to apologize for both its role in the Cambridge Analytica scandal and the confusion about user privacy, despite the fact that Facebook was aware that Cambridge Analytica exploited user data before the story was published?

Facebook did not wait until after *The Guardian*'s report about Cambridge Analytica to seek assurance that the data was deleted. Facebook contacted Cambridge Analytica immediately following *The Guardian* article in December 2015. About one month later, on January 18, 2016, Cambridge Analytica assured Facebook in writing that it had deleted the data received from Kogan/GSR and that its server contained no backups of the data.

c. Why did it take *The Guardian*'s reporting for Facebook to identify the problem with Alexandr Kogan and Cambridge Analytica?

Since 2014, Facebook has proactively reviewed any app seeking to obtain extended permissions to data beyond a basic set of data, and it has rejected more than half of the apps seeking these permissions. Before we learned about *The Guardian* allegations and through today, Facebook's policies regarding third-party usage of its platform technologies have prohibited—and continue to prohibit—third-party app developers from selling or licensing user data accessed from Facebook and from sharing any user data accessed from Facebook with any ad network, data broker or other advertising or monetization-related service. We take action on potential violations of our Platform Policies based on proactive review, external reports, and other signals.

d. How many of the changes that Facebook implemented this year should be credited to *The Guardian* and others' reporting?

See Response to Question 4(c).

e. Has Facebook previously threatened to sue a publication in regards to a news story?

See Response to Question 4(a).

f. Would Facebook support a Federal anti-SLAPP (strategic lawsuit against public participation) law in order to protect reporters and publications from censorship and intimidation?

As noted above, Facebook did not threaten to sue *The Guardian*. We sent *The Guardian* a letter to correct some facts in the article they sought to publish. Facebook supports vocal, independent journalism, and we would not threaten litigation to undermine the press or deter meaningful public discourse.

5. Privacy:

a. Does Facebook notify users of how an individual or entity who develops a Platform application plans to use user data?

In November 2013, when Kogan's app first became active on the platform, apps generally could be launched on the Facebook Platform without affirmative review or approval by Facebook. Kogan's app used the Facebook Login service, which allowed users to utilize their Facebook credentials to authenticate themselves to third-party services. Facebook Login and Facebook's Graph API also allowed Kogan's app to request permission from its users to access certain categories of data that users had entered into their Facebook profiles, as well as certain data their friends had shared with them, if enabled by these friends' privacy settings.

The App Review process introduced in 2014 requires developers who create an app that asks for more than certain basic user information from installers to justify the data they are looking to collect and how they are going to use it. Facebook then reviews whether the developer has a legitimate need for the data in light of how the app functions. Only if approved following

such review can the app ask for users' permission to get their data. Facebook has rejected more than half of the apps submitted for App Review between April 2014 and April 2018.

We are in the process of investigating every app that had access to a large amount of information before we changed our Platform in 2014. Where we have concerns, we will conduct interviews, make requests for information (RFI)—which ask a series of detailed questions about the app and the data it has access to—and perform audits that may include on-site inspections. If we determine that there has been improper use of data, we will ban those developers and notify everyone affected. Facebook is launching the Data Abuse Bounty to reward people who report any misuse of data by app developers. The Data Abuse Bounty, inspired by the existing bug bounty program that we use to uncover and address security issues, will help us identify violations of our policies.

Further, Facebook's Platform Policy makes clear to app developers the relevant requirements regarding users' privacy that apply to apps operating on the Platform, including the requirements to give users choice and control, and to respect user privacy. Application developers explicitly agree to Facebook's Statement of Rights and Responsibilities and Platform Policy when they set up their Facebook accounts. The Platform Policy imposes a variety of obligations on app developers regarding the features, functionality, data collection and usage, and content for apps on the Platform, as well as Facebook's right to take enforcement action if an application violates the Platform Policy.

b. If an individual or entity that creates an app for Facebook designates that they intend to use the user information acquired from that app for research, does Facebook notify the user of this planned use?

See Response to Question 5(a).

c. In cases in which Facebook relies on the app developer to notify users of how their data will be used, does Facebook verify that the developer is accurately representing how they will utilize user data? If so, how? If not, why not?

We use a variety of tools to enforce Facebook policies against violating parties, including developers. We review tens of thousands of apps per year and regularly disapprove noncompliant apps as part of our proactive review process. We also use tools like cease-and-desist letters, account suspensions, letter agreements, and civil litigation. For example, since 2006, Facebook has sent over 1,150 cease-and-desist letters to over 1,600 targets. In 2017, we took action against about 370,000 apps, ranging from imposing certain restrictions to removal of the app from the platform. Moreover, we have required parties who have procured our data without authorization to delete that data. We have invested significant resources in these efforts. Facebook is presently investigating apps that had access to large amounts of information before we changed our platform policies in 2014 to significantly reduce the data apps could access. As of early June 2018, around 200 apps (from a handful of developers: Kogan, AIQ, Cube You, the Cambridge Psychometrics Center, myPersonality, and AIQ) have been suspended—pending a thorough investigation into whether they did in fact misuse any data.

Additionally, we have suspended an additional 14 apps, which were installed by around one thousand people. They were all created after 2014, after we made changes to more tightly restrict our platform APIs to prevent abuse. However, these apps appear to be linked to AIQ, which was affiliated with Cambridge Analytica. So, we have suspended them while we investigate further. Any app that refuses to take part in or fails our audit will be banned.

d. Facebook announced that it is streamlining its privacy controls so that consumers can better understand how Facebook is using a person's data.

i Please describe what you are doing to your settings to be more transparent about your massive data collection and monetization operations.

ii Will you provide new default privacy settings for consumers?

We believe that it's important to communicate with people about the information that we collect and how people can control it. That is why we work hard to provide this information to people in a variety of ways: in our Data Policy, and in Privacy Basics, which provides walkthroughs of the most common privacy questions we receive. Beyond simply disclosing our practices, we also think it's important to give people access to their own information, which we do through our Download Your Information and Access Your Information tools, Activity Log, and Ad Preferences, all of which are accessible through our Privacy Shortcuts tool. We also provide information about these topics as people are using the Facebook service itself.

We've heard loud and clear that privacy settings and other important tools are too hard to find and that we must do more to keep people informed. So, we're taking additional steps to put people more in control of their privacy. For instance, we redesigned our entire settings menu on mobile devices from top to bottom to make things easier to find. We also created a new Privacy Shortcuts in a menu where users can control their data in just a few taps, with clearer explanations of how our controls work. The experience is now clearer, more visual, and easy-to-find. Furthermore, we also updated our terms of service that include our commitments to everyone using Facebook. We explain the services we offer in language that's easier to read. We also updated our Data Policy to better spell out what data we collect and how we use it in Facebook, Instagram, Messenger, and other products.

People own what they share on Facebook, and they can manage things like who sees their posts and the information they choose to include on their profile.

Any person can see each of the specific interests we maintain about them for advertising by visiting Ads Preferences, which lets people see what interests we use to choose ads for them—and to edit or delete these interests. They can choose not to see ads from a particular advertiser or not to see ads based on their use of third-party websites and apps. They also can choose not to see ads off Facebook that are based on the interests we derive from their activities on Facebook.

Our Download Your Information or "DYI" tool is Facebook's data portability tool and was launched many years ago to let people access and download many types of information that we maintain about them. The data in DYI and in our Ads Preferences tool contain each of the

interest categories that are used to show people ads, along with information about the advertisers that are currently running ads based on their use of an advertiser's website or app. People also can choose not to see ads from those advertisers. We recently announced expansions to Download Your Information, which, among other things, will make it easier for people to see their data, delete it, and easily download and export it. More information is available at https://newsroom.fb.com/news/2018/04/new-privacy-protections/.

And we recently announced plans to build Clear History. This feature will enable users to see the websites and apps that send us information when they use them, clear this information from their accounts, and turn off our ability to store it associated with their accounts going forward. Apps and websites that use features such as the Like button or Facebook Analytics send us information to make their content and ads better. We also use this information to make users' experiences on Facebook better. If a user clears their history or uses the new setting, we'll remove identifying information so a history of the websites and apps they've used won't be associated with their account. We'll still provide apps and websites with aggregated analytics—for example, we can build reports when we're sent this information so we can tell developers if their apps are more popular with men or women in a certain age group. We can do this without storing the information in a way that's associated with a user's account, and as always, we don't tell advertisers who a user is.

6. Additional user data: Mr. Zuckerberg, data that users voluntarily provide about themselves is not the only kind of user data that Facebook collects or uses to target ads.

a. What kind of inferences does Facebook make from data that users voluntarily upload?

We use data about things people do on Facebook, such as the Pages they like, to associate "interests" with their accounts, and we enable advertisers to reach audiences—i.e., groups of people—that share those interests. For example, if a person has liked Pages about baseball, we might associate them with interests called "baseball" or "sports."

We use data from devices (such as location data) to help advertisers reach people in particular areas. For example, if people have shared their device locations with Facebook or checked into a specific restaurant, we can show them ads from an advertiser that wants to promote its services in their area or from the restaurant.

In addition to general controls—such as Activity Log—we provide controls that specifically govern the use of data for ads. Through Ad Preferences, people see and control things like: (1) their "interests," which are keywords associated with a person based on activities such as liking Pages and clicking ads; (2) their "behaviors" (which we also call "categories"), which generally reflect how, when and where they connect to Facebook; and (3) the advertisers that are currently showing them ads based on the person's contact information, based on the person's previous use of the advertiser's website or app, or based on a visit to the advertiser's store. People also can choose whether we use information about their activities on websites and apps off of Facebook to show them ads through Facebook, and whether we can use their Facebook advertising interests to show them ads off of Facebook. People's use of these controls will, of course, affect the data we use to show them ads.

b. How does Facebook determine a user's political inclination when a user has not overtly selected political preference?

We enable ad targeting options—called "interests" and "behaviors"—that are based on people's activities on Facebook, and if enabled, information we receive from partners off Facebook. These options do not reflect people's personal characteristics, but we still take precautions to limit the potential for advertisers to misuse them. For example, we do not create interest or behavior segments that suggest the people in the segment are members of sensitive groups.

c. What data points does Facebook collect from non-Facebook sites?

When people visit apps or websites that feature our technologies—like the Facebook Like or Comment button—our servers automatically log (i) standard browser or app records of the fact that a particular device or user visited the website or app (this connection to Facebook's servers occurs automatically when a person visits a website or app that contains our technologies, such as a Like button, and is an inherent function of internet design); and (ii) any additional information the publisher of the app or website chooses to share with Facebook about the person's activities on that site (such as the fact that a purchase was made on the site). This is a standard feature of the internet, and most websites and apps share this same information with multiple different third-parties whenever people visit their website or app. For example, the House Energy and Commerce Committee's website shares information with Google Analytics to help improve the site. This means that, when a person visits the Committee's website, it sends browser information about their visit to each one of those third parties. More information about how this works is available at https://newsroom.fb.com/news/2018/04/data-off-facebook/.

When the person visiting a website featuring Facebook's tools is not a registered Facebook user, Facebook does not have information identifying that individual, and it does not create profiles for this individual.

We use the browser and app logs that apps and websites send to us—described above—in the following ways for non-Facebook users. First, these logs are critical to protecting the security of Facebook and to detecting or preventing fake account access. For example, if a browser has visited hundreds of sites in the last five minutes, that's a sign the device might be a bot, which would be an important signal of a potentially inauthentic account if that browser then attempted to register for an account. Second, we aggregate those logs to provide summaries and insights to websites and apps about how many people visit or use their product, or use specific features like our Like button—but without providing any information about a specific person. We do not create profiles for non-Facebook users, nor do we use browser and app logs for non-Facebook users to show targeted ads from our advertisers to them or otherwise seek to personalize the content they see. However, we may take the opportunity to show a general ad that is unrelated to the attributes of the person or an ad encouraging the non-user to sign up for Facebook.

When the individual is a Facebook user, we are also able to use this information to personalize their experiences on Facebook, whether or not they are logged out, but we will not target ads to users relying on this information unless the user allows this in their privacy settings. We do not sell or share this information with third-parties.

We do receive some information from devices and browsers that may be used by non-users. For example:

- We also may receive information about the device of a non-registered user if that user visits a part of Facebook that does not require people to log in—such as a public Facebook Page. The information we log when people visit our websites or apps is the same as described above and is the same information that any provider of an online service would receive.

- In addition, Facebook may receive some basic information about devices where Facebook apps are installed, including before people using those devices have registered for Facebook (such as when a user downloads a Facebook app, but has not yet created an account, or if the app is preloaded on a given device). This device data includes things like device model, operating system, IP address, app version and device identifiers. We use this information to provide the right version of the app, help people who want to create accounts (for example, optimizing the registration flow for the specific device), retrieving bug fixes and measuring and improving app performance. We do not use this information to build profiles about non-registered users.

d. What are these data points used for?

Our Data Policy describes in detail what we do with the information we receive. There are three main ways in which Facebook uses the information we get from other websites and apps: providing our services to these sites or apps; improving safety and security on Facebook; and enhancing our own products and services.

- Providing Our Services

    - *Social plugins and Facebook Login.* We use a person's IP address, browser/operating system information, and the address of the website or app they are using to make these features work. For example, knowing the IP address allows us to send the Like button to the person's browser and helps us show it in the person's language. Cookies and device identifiers help us determine whether the person is logged in, which makes it easier to share content or use Facebook to log into another app.

    - *Facebook Analytics.* Facebook Analytics (https://analytics.facebook.com/) gives websites and apps data about how they are used. IP addresses help us list the countries where people are using an app. Browser and operating system information enable us to give developers information about the platforms people use to access their app. Cookies and other identifiers help us count the number of unique visitors. Cookies also help us recognize which visitors are Facebook users so we can provide aggregated demographic information, like age and gender, about the people using the app.

    - *Ads.* Facebook Audience Network enables other websites and apps to show ads from Facebook advertisers. When we get a request to show an Audience

Network ad, we need to know where to send it and the browser and operating system a person is using. Cookies and device identifiers help us determine whether the person uses Facebook. If they don't, we can show an ad encouraging them to sign up for Facebook. If they do, we'll show them ads from the same advertisers that are targeting them on Facebook. We can also use the fact that they visited a site or app to show them an ad from that business—or a similar one—back on Facebook.

- *Ad Measurement.* An advertiser can choose to add the Facebook Pixel, some computer code, to their site. This allows us to give advertisers stats about how many people are responding to their ads—even if they saw the ad on a different device—without us sharing anyone's personal information.

- Keeping Your Information Secure

  - We also use the information we receive from websites and apps to help protect the security of Facebook. For example, receiving data about the sites a particular browser has visited can help us identify bad actors. If someone tries to log into an account using an IP address from a different country, we might ask some questions to verify it's the right person. Or if a browser has visited hundreds of sites in the last five minutes, that's a sign the device might be a bot. We'll ask them to prove they're a real person by completing additional security checks.

- Improving Our Products and Services

  - The information we receive also helps us improve the content and ads we show on Facebook. So if a person visits a lot of sports sites that use our services, you might see sports-related stories higher up in your News Feed. If you've looked at travel sites, we can show you ads for hotels and rental cars.

When the person visiting a website featuring Facebook's tools is not a registered Facebook user, Facebook does not have information identifying that individual, and it does not create profiles for this individual.

e. Why do these inferences and data points not appear when a user downloads their information from Facebook?

Our Download Your Information or "DYI" tool is Facebook's data portability tool and was launched many years ago to let people access and download many types of information that we maintain about them. The data in DYI and in our Ads Preferences tool contain each of the interest categories that are used to show people ads, along with information about the advertisers that are currently running ads based on their use of an advertiser's website or app. People also can choose not to see ads from those advertisers. We recently announced expansions to Download Your Information, which, among other things, will make it easier for people to see their data, delete it, and easily download and export it. More information is available at https://newsroom.fb.com/news/2018/04/new-privacy-protections/.

Responding to feedback that we should do more to provide information about websites and apps that send us information when people use them, we also announced plans to build Clear History. This new feature will enable users to see the websites and apps that send us information when they use them, clear this information from their account, and turn off Facebook's ability to store it associated with their account going forward.

We have also introduced Access Your Information. This feature provides a new way for people to access and manage their information. Users can go here to delete anything from their timeline or profile that they no longer want on Facebook. They can also see their ad interests, as well as information about ads they've clicked on and advertisers who have provided us with information about them that influence the ads they see. From here, they can go to their ad settings to manage how this data is used to show them ads.

f. Please clarify your response to Congressman McNemey's question: "Is there currently a place that I can download all of the Facebook information about me, including the websites that I have visited?", given that you responded affirmatively but then denied that the download includes information about websites the user has visited?

We are consistently working to improve our data access and portability tools. As stated in the hearing, the Download Your Information tool contains the content or information that you have provided to Facebook.

Responding to feedback that we should do more to provide information about websites and apps that send us information when people use them, we also announced plans to build Clear History. This new feature will enable users to see the websites and apps that send us information when they use them, clear this information from their account, and turn off Facebook's ability to store it associated with their account going forward.

We also recently published a post describing in detail the types of data we collect about people off of Facebook, including the websites they visit, to provide even more clarity on this point. The post is available here: https://newsroom.fb.com/news/2018/04/data-off-facebook/.

g. In your answer to Congressman McNerney's subsequent question, you said that Facebook does not have user browsing history. What does Facebook do with the browsing history Facebook collects?

i Why did you mislead the Committee by implying that Facebook does not have browsing history when it does collect browsing information? Please clarify.

See Response to Question 6(f).

h. Facebook compiles a wide range of data about individuals that have never signed up for a Facebook account, including such things as their hobbies and interests and what books they have read. How can an individual protect

their privacy if they are not a Facebook user and Facebook is compiling shadow profiles of them?

When the person visiting a website featuring Facebook's tools is not a registered Facebook user, Facebook does not have information identifying that individual, and it does not create profiles for this individual.

We use the browser and app logs that apps and websites send to us—described above in Question 6(c)—in the following ways for non-Facebook users. First, these logs are critical to protecting the security of Facebook and to detecting or preventing fake account access. For example, if a browser has visited hundreds of sites in the last five minutes, that's a sign the device might be a bot, which would be an important signal of a potentially inauthentic account if that browser then attempted to register for an account. Second, we aggregate those logs to provide summaries and insights to websites and apps about how many people visit or use their product, or use specific features like our Like button—but without providing any information about a specific person. We do not create profiles for non-Facebook users, nor do we use browser and app logs for non-Facebook users to show targeted ads from our advertisers to them or otherwise seek to personalize the content they see. However, we may take the opportunity to show a general ad that is unrelated to the attributes of the person or an ad encouraging the non-user to sign up for Facebook.

When the individual is a Facebook user, we are also able to use this information to personalize their experiences on Facebook, whether or not they are logged out, but we will not target ads to users relying on this information unless the user allows this in their privacy settings. We do not sell or share this information with third-parties.

We do receive some information from devices and browsers that may be used by non-users. For example:

- We also may receive information about the device of a non-registered user if that user visits a part of Facebook that does not require people to log in—such as a public Facebook Page. The information we log when people visit our websites or apps is the same as described above and is the same information that any provider of an online service would receive.

- In addition, Facebook may receive some basic information about devices where Facebook apps are installed, including before people using those devices have registered for Facebook (such as when a user downloads a Facebook app, but has not yet created an account, or if the app is preloaded on a given device). This device data includes things like device model, operating system, IP address, app version and device identifiers. We use this information to provide the right version of the app, help people who want to create accounts (for example, optimizing the registration flow for the specific device), retrieving bug fixes and measuring and improving app performance. We do not use this information to build profiles about non-registered users.

i. How can you guarantee that you are not collecting data about children who are not on Facebook and who are not able to guarantee that they are the minimum age of 13?

We do not knowingly collect info on minors.

When the person visiting a website featuring Facebook's tools is not a registered Facebook user, Facebook does not have information identifying that individual, and it does not create profiles for this individual.

The Honorable Scott Peters

1. Facebook's terms of service state that "you own all of the content and information you post on Facebook, and you can control how it is shared." Your consent decree with the FTC states Facebook "shall not misrepresent in any manner, expressly or by implication, the extent to which it maintains the privacy or security of covered information." Doesn't this statement in the TOS erroneously lead the 87 million users who had no idea their data was being analyzed by Cambridge Analytica into believing that they had control and ownership over which third parties could access their Facebook information?

In 2011, Facebook offered more control and protection over the availability of friends' data to apps than any other digital platform at the time, including mobile app platforms, which generally permitted apps to access user data and their friends' data without consent or any control. By contrast, Facebook notified users of each category of data an app could access—including friends data—before the user consented to the app, and also provided all users with controls that would prevent their friends from sharing their data with apps on Facebook's platform.

We furnished extensive information to the FTC regarding the ability for users to port their Facebook data (including friends data that had been shared with them) with apps on Facebook's platform, as part of the FTC's investigation culminating in the July 27, 2012 Consent Order. The Consent Order memorializes the agreement between Facebook and the FTC and did not require Facebook to turn off the ability for people to port friends data that had been shared with them on Facebook to apps they used. Facebook voluntarily changed this feature of the Platform in 2014, however.

Among other things, the Consent Order obligates Facebook not to misrepresent the extent to which it maintains the privacy or security of covered information (Section I), not to materially exceed the restrictions of a privacy setting that applies to nonpublic user information without affirmative express consent (Section II), and to implement a comprehensive privacy program that is subjected to ongoing review by an independent assessor (Sections IV and V). Facebook accurately represented the operation of its developer Platform and the circumstances under which people could share data (including friends data) with developers, honored the restrictions of all privacy settings that covered developer access to data, and implemented a comprehensive privacy program built on industry-leading controls and principles, which has undergone ongoing review by an independent assessor approved by the FTC.

The Honorable Debbie Dingell

1. When a Pixel sends general browsing session information back to Facebook servers, is that connection HTTP or HTTPS?

The Facebook Pixel is designed to use https connections by default. Websites are in control of the specific pixel addresses that they place on their webpages, but if we receive a pixel call through an http connection, we will redirect the browser to an https connection.

2. If information is sent clear-text via HTTP, do you have plans to move to the more secure HTTPS?

In 2011, we gave people the option to select https as the default for their Facebook connections, and in 2013 we introduced this as the default for all Facebook users.

3. On websites that offer the Log in with Facebook feature, third parties can embed JavaScript to grab data from the Facebook API and collect items such as hashed and unhashed Facebook User ID, hashed and unhashed email, and gender. Is Facebook aware that such practices are taking place?

We understand you to be referring to this *TechCrunch* report: https://techcrunch.com/2018/04/18/login-with-facebook-data-hijacked-by-javascript-trackers/. We have taken immediate action by suspending the ability to link unique user IDs for specific applications to individual Facebook profile pages except by people who either are already in the individual's extended network or who are using apps that have entered into restrictive agreements with Facebook.

4. And if so, what is Facebook doing to curb unauthorized third-party code embedded on sites with Facebook Login from collecting users profile information when they create accounts?

See Response to Question 3.

5. Your quick response to my questions with the number of Like and Share buttons and pixel installations were appreciated. In your response you said the Like button appeared on 8.4 million websites, covering 2.6 billion webpages, the Share button was on 931,000 websites covering 275 million pages, and the pixel was installed on 2.2 million websites. What is the percentage of total web traffic where Facebook have a pixel, like button, or share button present?

Facebook does not know how much web traffic is created in total.

6. Other than for routing or functionality purposes, does Facebook conduct any deep packet inspection of traffic traversing the undersea cable Marea or any other internet backbone infrastructure?

We do not perform deep packet inspection on traffic traversing Marea or any other network backbone infrastructure.

House Energy and Commerce Committee

Hearing Follow-up Questions

Rep. Bilirakis

I think the solution to the opioid question you mentioned earlier of doing more with automated tools will lead to both faster response times and more accurate enforcement of the policies. Can you give us a timeline as to when will this be done?

Our effort to make our platform safer and more secure is a holistic one that involves a continual evaluation of our personnel, processes, and policies, and we make changes as appropriate. We are doubling the size of our security and content review teams (from 10,000 to 20,000) over the course of this year. We currently have approximately 15,000 people working on these teams. The team also includes specialists in areas like child safety, hate speech and counter-terrorism, software engineers to develop review systems, quality control managers, policy specialists, legal specialists, and general reviewers.

We employ a mix of full-time employees, contractors and vendor partners to assist with content review and help us scale globally. Our content review team is global, reviews reports in over 50 languages, 24 hours a day, 7 days a week and the vast majority of reports are reviewed within 24 hours. Our goal is always to have the right number of skilled people with the right language capabilities to help ensure incoming reports are reviewed quickly and efficiently. We hire people with native language and other specialist skills according to the needs we see from incoming reports. We partner with reputable vendors who are required to comply with specific obligations, including provisions for resiliency, support, transparency, and user privacy.

We are also using machine learning to better detect and action on content and people that should not be using our platform, across all abuse types, including illegal drug sales. We recently shared how we are using machine learning to prevent bad actors like terrorists or scammers from using our platform (https://www.facebook.com/notes/facebook-security/introducing-new-machine-learning-techniques-to-help-stop-scams/10155213964780766/).

Rep. Butterfield

So will you commit, sir, to convene personally convene a meeting of CEOs in your sectors, many of them, all of them perhaps, are your friends and to do this very quickly to develop a strategy to increase racial diversity in the technology industry?

Relman, Dane & Colfax, a respected civil rights law firm, will carry out a comprehensive civil rights assessment of Facebook's services and internal operations. Laura Murphy, a national civil liberties and civil rights leader, will help guide this process—getting feedback directly from civil rights groups, like The Leadership Conference on Civil and Human Rights, and help advise Facebook on the best path forward.

With a global community of over two billion people on Facebook, greater diversity and inclusivity are critical to achieving our mission. Studies have shown that cognitive diversity on teams that are working on hard problems produces better results. Diversity helps us build better products, make better decisions and better serve our community. In order to achieve that, we have developed programming to attract and retain more people from traditionally underrepresented groups which include women, people of color, veterans and people with disabilities.

We are not where we would like to be, but we are encouraged that representation for people from underrepresented groups at Facebook has increased. We've grown Black and Hispanic representation by 1 percent each (2 percent combined) between our first report in 2014 and our most recent report in 2017 (note that ethnicity data is for US employees):

- Black Representation: from 2 percent to 3 percent
- Hispanic Representation: from 4 percent to 5 percent
- Black Non-Tech: from 2 percent to 6 percent
- Hispanic Non-Tech: from 6 percent to 8 percent
- Black Leadership: from 2 percent to 3 percent
- Hispanic Leadership: from 4 percent to 3 percent
- Black and Hispanic Tech have stayed at 1 percent and 3 percent

As of August 2017, the number of women globally increased from 33 percent to 35 percent:

- Women in Tech: from 17 percent to 19 percent
- Women in Non-Tech: from 47 percent to 55 percent
- Women in Leadership: from 23 percent to 28 percent
- Women made up 27 percent of all new graduate hires in engineering and 21 percent of all new technical hires at Facebook.

We seek to promote diversity in a variety of ways, and we want to highlight three programs in particular. First, we have adopted our Diverse Slate Approach (DSA) to interviewing job candidates. The more people that hirers interview who don't look or think like them, the more likely they are to hire someone from a diverse background. To hardwire this behavior at Facebook, we introduced our DSA in 2015 and have since rolled it out globally. DSA

sets the expectation that hiring managers will consider candidates from underrepresented backgrounds when interviewing for an open position.

Second, we are working to reduce unconscious bias. Our publicly available Managing Unconscious Bias class encourages our people to challenge and correct bias as soon as they see it—in others, and in themselves. We've also doubled down by adding two additional internal programs: Managing Inclusion, which trains managers to understand the issues that affect marginalized communities, and Be The Ally, which gives everyone the common language, tools, and space to practice supporting others.

Third, we have created Facebook University. We want to increase access and opportunity for students with an interest in software engineering, business, and analytics. Facebook University (FBU) gives underrepresented students extra training and mentorship earlier in their college education. We started FBU in 2013 with 30 students and expect to have 280 in 2018. More than 500 students have graduated from this program, with many returning to Facebook for internships and full-time jobs.

Finally, we have many partnerships to move the numbers nationally such as Black Girls Code, All Star Code, Hack the Hood, The Hidden Genius Project, Level Playing Field Institute, Yes We Code, Streetcode Academy, Dev Color, Dev Bootcamp and Techbridge. And, we now recruit at 300 Universities—including historically black colleges and universities (HBCUs) like Spelman, Morehouse, Howard, NCA&T, and Morgan State (EIR) and the HBCU Faculty Summit.

We're committed to building a more diverse, inclusive Facebook. Much like our approach to launching new products on our platform, we are willing to experiment and listen to feedback.

Rep. Dingell

How many Facebook like buttons are there on non-Facebook web pages? How many Facebook share buttons are there on non Facebook web pages? How many chunks of Facebook pixel code are there on non-Facebook web pages?

During the week prior to April 16, 2018, on sites that use Facebook services, the Like button appeared on 8.4 million websites, the Share button on 931,000 websites covering 275 million webpages, and there were 2.2 million Facebook pixels installed on websites.

Facebook does not publish tracking software. When people visit apps or websites that feature our technologies—like the Facebook Like or Comment button—our servers automatically log (i) standard browser or app records of the fact that a particular device or user visited the website or app (this connection to Facebook's servers occurs automatically when a person visits a website or app that contains our technologies, such as a Like button, and is an inherent function of internet design); and (ii) any additional information the publisher of the app or website chooses to share with Facebook about the person's activities on that site (such as the fact that a purchase was made on the site). This is a standard feature of the internet, and most websites and apps share this same information with multiple different third-parties whenever people visit their website or app. For example, the House Energy and Commerce Committee's website shares information with Google Analytics to help improve the site. This means that, when a person visits the Committee's website, it sends browser information about their visit to that third party. More information about how this works is available at https://newsroom.fb.com/news/2018/04/data-off-facebook/.

Rep. Engel

Mark Zuckerberg: We are doing a number of things that I'm happy to talk about or follow up with afterwards around deploying new AI tools that can proactively catch fake accounts that Russia or others might create to spread misinformation, buy political ads, or interfere in an election.

We are committed to finding and removing fake accounts. We continue to make improvements to our efforts to more effectively detect and deactivate fake accounts to help reduce the spread of spam, false news, and misinformation. We continually update our technical systems to identify, checkpoint, and remove inauthentic accounts, and we block millions of attempts to register fake accounts every day. These systems examine thousands of detailed account attributes and prioritize signals that are more difficult for bad actors to disguise, such as their connections to others on our platform. As with all security threats, we have been incorporating new insights into our models for detecting fake accounts, including information specific to election issues.

We do not share detailed descriptions of how our tools work in order to avoid providing a road map to bad actors who are trying to avoid detection. When we suspect that an account is inauthentic, we typically enroll the account in a checkpoint that requires the account holder to provide additional information or verification. We view disabling an account as a severe sanction, and we want to ensure that we are highly confident that the account violates our policies before we take permanent action. When we have confirmed that an account violates our policies, we remove the account.

Rep. Flores

Do you agree that Facebook and other technology platforms should be ideologically neutral?

Facebook is a community, and we want people to feel confident that our community welcomes all viewpoints. We are committed to designing our products to give all people a voice and foster the free flow of ideas and culture. Diversity in all its forms—including ideological—is one of our core values, and we believe that adding voices to the conversation creates a richer and more vibrant community.

You said each user owns their virtual presence. Do you think this concept should apply to all social media providers, including internet providers and ISPs?

Facebook believes that the data users share with Facebook is their data and has taken steps to make it easier for users to access and manage that data. We work hard to provide clear information to people about how their information is used and how they can control it. We agree that companies should provide clear and plain information about their use of data and strive to do this in our Data Policy, in in-product notices and education, and throughout our product—and we continuously work on improving this.

Rep. Green

GDPR also gives users the right to object to the process of their personal data for marketing purposes, which according to Facebook's website includes custom microtargeted audiences for advertising. Will the same right be—to object be available to Facebook users in the united states and how will that be implemented?

As a part of our overall approach to privacy, we are providing the same tools for access, rectification, erasure, data portability, and others to people in the US (and globally) that we provide in the European Union under the GDPR. The controls and settings that Facebook is enabling as part of GDPR include settings for controlling our use of face recognition on Facebook and for controlling our ability to use data we collect off Facebook Company Products to target ads. We recently began providing direct notice of these controls and our updated terms to people around the world (including in the US), allowing people to choose whether or not to enable or disable these settings or to consent to our updated terms. Many of these tools (like our Download Your Information tool, ad preferences tool, and Activity Log) have been available globally for many years.

The substantive protections in our user agreements offered by Facebook Ireland and Facebook, Inc. are the same. However, there are certain aspects of our Facebook Ireland Data Policy that are specific to legal requirements in the GDPR—such as the requirement that we provide contact information for our EU Data Protection Officer or that we identify the "legal bases" we use for processing data under the GDPR. Likewise, our Facebook Ireland terms and Data Policy address the lawful basis for transferring data outside the EU, based on legal instruments that are applicable only to the EU. And other provisions of the GDPR itself pertain to interactions between European regulators and other matters that are not relevant to people located outside of the EU.

Facebook is subject to ongoing oversight by the Federal Trade Commission with respect to its privacy commitments to people and its implementation of privacy settings, under a Consent Order with the FTC. Facebook is subject to the authority of the Irish Data Protection Commissioner, its lead regulator, under the GDPR in the European Union.

We do not use web browsing data to show ads to non-users or otherwise store profiles about non-users. Our goal is to show people content (including advertising) that is relevant to their interests. We use information people have provided on Facebook—such as things they've liked or posts they've engaged with—to help determine what people will be interested in. Like most online advertising companies, we also inform our judgments about what ads to show based on apps and websites that people use off of Facebook. People can turn off our use of web browser data and other data from third-party partners to show them ads through a control in Ads Preferences. They can also customize their advertising experience by removing interests that they do not want to inform the Facebook ads they see. In addition, a person's browser or device may offer settings that allow users to choose whether browser cookies are set and to delete them.

Rep. Hudson

Are you aware of the national security concerns that come from allowing those who seek to harm our nation such a geographic call location of members of our armed services? Is this something you're looking at?

We are aware that threat actors seek to leverage social media to target military personnel. We have a threat intelligence team dedicated to countering these sorts of cybersecurity threats, and we are expanding that team along with other teams that work on safety and security at Facebook. Many of the security features on Facebook that protect our users from abusive targeting are equally available to members of the military. For example, we provide guidance on performing a security checkup, and we prevent malicious files from being uploaded or shared by users. In addition, we partnered with Blue Star Families and USAA to create an online safety guide specifically for service members and their families—and recently released a video PSA (https://www.facebook.com/FBMilVetCommunity/videos/1655416797877942/) to help people identify and report military scams. We regularly train and advise military officials on best practices for maintaining secure accounts and Pages, which includes setting up two-factor authentication and managing Page Roles. And of course, military personnel, like all Facebook users, have the ability to control who sees their Posts and other information.

Rep. Johnson

What happened to the person that took down the Franciscan university ad and didn't put it back up until the media started getting involved?

We acknowledge that this ad was improperly rejected. The content was restored as soon as we became aware of the error. The ad was disapproved for approximately 79 hours.

We recognize that our policies are only as good as the strength and accuracy of our enforcement—and our enforcement is not perfect. When we're made aware of incorrect content removals, we review them with team members to prevent similar mistakes in the future. We also audit the accuracy of reviewer decisions on an ongoing basis to coach them and follow up on improving, where errors are being made.

Additionally, we recently launched an appeals process that will enable people to request review of our content decisions. Prior to April 24, 2018, appeals generally were only available to people whose profiles, Pages, or Groups had been taken down, but we had not yet been able to implement an appeals process at the content level. On April 24, we announced the launch of appeals for content that was removed for nudity/sexual activity, hate speech, and graphic violence. We focused on starting with these content violations initially based on feedback from our community. We are working to extend this process further, by: supporting more violation types; giving people the opportunity to provide more context that could help us make the right decision; and making appeals available not just for content that was taken down, but also for content that was reported and left up.

Reps. Johnson, Loebsack, Capito, Griffith

What is Facebook doing to improve broadband in rural areas?

Facebook's ability to build communities and bring the world closer together depends on people being connected. Communities come in all sizes and across all regions, but many aren't currently being served by traditional methods of connectivity. Urban areas don't have enough bandwidth to support more devices running more data-heavy experiences, while in remote communities the technology is often too expensive to deploy. Through Facebook's connectivity efforts, we're working to help change that.

We're focused on developing next-generation technologies that can help bring the cost of connectivity down to reach the unconnected and increase capacity and performance for everyone else. We know that there is no silver bullet for connecting the world; no single technology or program will get the job done. Rather than look for a one-size-fits-all solution, we are investing in a building block strategy—designing different technologies for specific use cases which are then used together to help connect the approximately 3.8 billion people without access to internet.

We would be happy to brief your staff on these efforts.

Rep. Kennedy

You focus a lot of your testimony and the questions on the individual privacy aspects of this, but we haven't talked about the societal implication of it, and I think while I applaud some of the reforms that you're putting forward, the underlying issue here is that your platform has become a mix of news, entertainment, social media, that is up for manipulation. We've seen that with a foreign actor. If the changes to individual privacy don't seem to be sufficient to address that underlying issue. Would love your comments on that at the appropriate time.

Facebook is committed to protecting its platform from bad actors, ensuring Facebook is able to continue its mission of giving people a voice and bringing them closer together. And Facebook has been undertaking various efforts towards this goal. Facebook's security team has been aware of traditional Russian cyber threats for years and has actively investigated and responded to these concerns. For example, Facebook is committed to enforcing authenticity and has removed numerous Facebook and Instagram accounts that are controlled by foreign actors, like the Internet Research Agency. Facebook's security team has also identified new threats, like APT28 and DC Leaks, and shut down these accounts for violating Facebook policies. Facebook is also actively building new technologies to help prevent abuse on its platform, including advanced AI tools to monitor and remove fake accounts. Facebook has also significantly increased its investment in security, employing more than 15,000 individuals working solely on security and content review and planning to increase that number to over 20,000 by the end of the year.

Rep. Kinzinger

What personal data does Facebook make available from Facebook, Instagram, WhatsApp to Russian state agencies, including intel and security agencies?

As part of official investigations, government officials sometimes request data about people who use Facebook. We have strict processes in place to handle these government requests, and we disclose account records solely in accordance with our terms of service and applicable law. We require officials to provide a detailed description of the legal and factual basis for their request, and we push back if the request appears to be legally deficient or is overly broad, vague, or otherwise inconsistent with our policies. Further, with respect to government requests for disclosure from outside the United States, a Mutual Legal Assistance Treaty request or letter rogatory may be required to compel the disclosure of the contents of an account.

As part of our ongoing effort to share information about the requests we have received from governments around the world, Facebook regularly produces a Transparency Report about government data requests to Facebook. Our Transparency Report contains historical information about Russian requests for data going back to 2013. In summary, we received 34 requests from the Russian government between 2013 and 2017. We did not provide any data in response to these requests. See https://transparency.facebook.com/government-data-requests/country/RU.

Rep. Lance

Might I respectfully request of you, Mr. Zuckerberg, that you and your company review the BROWSER legislation, and I would like your support for that legislation after your review of it.

Facebook is generally not opposed to regulation but wants to ensure it is the right regulation. The issues facing the industry are complex, multi-faceted, and affect an important part of peoples' lives. As such Facebook is absolutely committed to working with policymakers, like Congress, to craft the right regulations. As requested, we will follow up with your staff to provide specific feedback on the BROWSER Act.

Rep. Blackburn

Will you commit to working with us to pass privacy legislation, to pass the BROWSER Act? Will you commit to doing that?

Facebook is generally not opposed to regulation but wants to ensure it is the right regulation. The issues facing the industry are complex, multi-faceted, and affect an important part of peoples' lives. As such Facebook is absolutely committed to working with policymakers, like Congress, to craft the right regulations. As requested, we will follow up with your staff to provide specific feedback on the BROWSER Act.

Rep. Lujan

Do you know how many points of data Facebook has on the average non-Facebook user?

When people visit apps or websites that feature our technologies—like the Facebook Like or Comment button—our servers automatically log (i) standard browser or app records of the fact that a particular device or user visited the website or app (this connection to Facebook's servers occurs automatically when a person visits a website or app that contains our technologies, such as a Like button, and is an inherent function of internet design); and (ii) any additional information the publisher of the app or website chooses to share with Facebook about the person's activities on that site (such as the fact that a purchase was made on the site). This is a standard feature of the internet, and most websites and apps share this same information with multiple different third-parties whenever people visit their website or app. For example, the House Energy and Commerce Committee's website shares information with Google Analytics to help improve the site. This means that, when a person visits the Committee's website, it sends browser information about their visit to that third party. More information about how this works is available at https://newsroom.fb.com/news/2018/04/data-off-facebook/.

When the person visiting a website featuring Facebook's tools is not a registered Facebook user, Facebook does not have information identifying that individual, and it does not create profiles for this individual.

We use the browser and app logs that apps and websites send to us—described above—in the following ways for non-Facebook users. First, these logs are critical to protecting the security of Facebook and to detecting or preventing fake account access. For example, if a browser has visited hundreds of sites in the last five minutes, that's a sign the device might be a bot, which would be an important signal of a potentially inauthentic account if that browser then attempted to register for an account. Second, we aggregate those logs to provide summaries and insights to websites and apps about how many people visit or use their product or use specific features like our Like button—but without providing any information about a specific person. We do not create profiles for non-Facebook users, nor do we use browser and app logs for non-Facebook users to show targeted ads from our advertisers to them or otherwise seek to personalize the content they see. However, we may take the opportunity to show a general ad that is unrelated to the attributes of the person or an ad encouraging the non-user to sign up for Facebook.

We do receive some information from devices and browsers that may be used by non-users. For example:

- We also may receive information about the device of a non-registered user if that user visits a part of Facebook that does not require people to log in—such as a public Facebook Page. The information we log when people visit our websites or apps is the same as described above and is the same information that any provider of an online service would receive.

- In addition, Facebook may receive some basic information about devices where Facebook apps are installed, including before people using those devices have registered

for Facebook (such as when a user downloads a Facebook app, but has not yet created an account, or if the app is preloaded on a given device). This device data includes things like device model, operating system, IP address, app version and device identifiers. We use this information to provide the right version of the app, help people who want to create accounts (for example, optimizing the registration flow for the specific device), retrieving bug fixes and measuring and improving app performance. We do not use this information to build profiles about non-registered users.

Rep. McMorris-Rodgers

In November FCC chairman Pai even said that edge providers routinely block or discriminate against content they don't like. This is obviously a serious allegation. How would you respond to such an allegation and what is Facebook doing to ensure that its users are being treated fairly and objectively by content reviewers?

Being a platform for all ideas is a foundational principle of Facebook. We are committed to ensuring there is no bias in the work we do.

Suppressing content on the basis of political viewpoint or preventing people from seeing what matters most to them is directly contrary to Facebook's mission and our business objectives.

When allegations of political bias surfaced in relation to Facebook's Trending Topics feature, we immediately launched an investigation to determine if anyone violated the integrity of the feature or acted in ways that are inconsistent with Facebook's policies and mission. We spoke with current reviewers and their supervisors, as well as a cross-section of former reviewers; spoke with our contractor; reviewed our guidelines, training, and practices; examined the effectiveness of operational oversight designed to identify and correct mistakes and abuse; and analyzed data on the implementation of our guidelines by reviewers.

Ultimately, our investigation revealed no evidence of systematic political bias in the selection or prominence of stories included in the Trending Topics feature. In fact, our analysis indicated that the rates of approval of conservative and liberal topics are virtually identical in Trending Topics. Moreover, we were unable to substantiate any of the specific allegations of politically-motivated suppression of subjects or sources, as reported in the media. To the contrary, we confirmed that most of those subjects were in fact included as trending topics on multiple occasions, on dates and at intervals that would be expected given the volume of discussion around those topics on those dates.

Nonetheless, as part of our commitment to continually improve our products and to minimize risks where human judgment is involved, we are making a number of changes:

- We have engaged an outside advisor, former Senator Jon Kyl, to advise the company on potential bias against conservative voices. We believe this external feedback will help us improve over time and ensure we can most effectively serve our diverse community and build trust in Facebook as a platform for all ideas.

- We continue to expand our list of outside partner organizations to ensure we receive feedback on our content policies from a diverse set of viewpoints.

- We have made our detailed reviewer guidelines public to help people understand how and why we make decisions about the content that is and is not allowed on Facebook.

- We have launched an appeals process to enable people to contest content decisions with which they disagree.

- We are instituting additional controls and oversight around the review team, including robust escalation procedures and updated reviewer training materials.

- These improvements and safeguards are designed to ensure that Facebook remains a platform for all ideas and enables the broadest spectrum of free expression possible.

To reduce the spread of false news, one of the things we're doing is working with third-party fact checkers to let people know when they are sharing news stories (excluding satire and opinion) that have been disputed or debunked, and to limit the distribution of stories that have been flagged as misleading, sensational, or spammy. Third-party fact-checkers on Facebook are signatories to the non-partisan International Fact-Checking Network Code of Principles. Third-party fact-checkers investigate stories in a journalistic process meant to result in establishing the truth or falsity of the story.

With respect to News Feed, a user's News Feed is made up of stories from their friends, Pages they've chosen to follow, and groups they've joined. Ranking is the process we use to organize all of those stories so that users can see the most relevant content at the top, every time they open Facebook. Ranking has four elements: the available inventory of stories; the signals, or data points that can inform ranking decisions; the predictions we make, including how likely we think a user is to comment on a story, share with a friend, etc.; and a relevancy score for each story.

News Feed considers thousands of signals to surface the content that's most relevant to each person who uses Facebook. Our employees don't determine the ranking of any specific piece of content. To help the community understand how News Feed works and how changes to News Feed affect their experience on Facebook, we publish a regularly-updated News Feed FYI blog (https://newsroom.fb.com/news/category/inside-feed/) where our team shares details of significant changes.

Rep. McNerney

Is there any other information that Facebook has obtained about me whether Facebook collected it or obtained it from a third party that would not be included in the download?

Our Download Your Information or "DYI" tool is Facebook's data portability tool and was launched many years ago to let people access and download many types of information that we maintain about them. The data in DYI and in our Ads Preferences tool contain each of the interest categories that are used to show people ads, along with information about the advertisers that are currently running ads based on their use of an advertiser's website or app. People also can choose not to see ads from those advertisers. We recently announced expansions to Download Your Information, which, among other things, will make it easier for people to see their data, delete it, and easily download and export it. More information is available at https://newsroom.fb.com/news/2018/04/new-privacy-protections/.

Responding to feedback that we should do more to provide information about websites and apps that send us information when people use them, we also announced plans to build Clear History. This new feature will enable users to see the websites and apps that send us information when they use them, clear this information from their account, and turn off Facebook's ability to store it associated with their account going forward.

We have also introduced Access Your Information. This feature provides a new way for people to access and manage their information. Users can go here to delete anything from their timeline or profile that they no longer want on Facebook. They can also see their ad interests, as well as information about ads they've clicked on and advertisers who have provided us with information about them that influence the ads they see. From here, they can go to their ad settings to manage how this data is used to show them ads.

Rep. Pallone

Will you make the commitment to changing all the user default settings to minimize to the greatest extent possible the collection and use of user's data?

We regularly review and update our settings to help people protect their privacy and give people choices about how their information is used and who can see it. That's why, for example, in 2014 we changed the default audience for posts from Public to Friends, and why we now ask people when they create a new account who they would like to see the things they post—their friends, the public, or a different audience.

Rep. Peters

[Regarding AI development] There are examples of how decisions are made on a discriminatory basis. They can compound if you are not careful about how that occurs. As your company, is your company developing a set of principles that are going to guide that development? Can you provide details to us about what those principles are and how they will help deal with those issues?

We are focused on both the technical and the ethical aspects of artificial intelligence. We believe these two should go hand-in-hand together in order to fulfill our commitment to being fair, transparent and accountable in our development and use of AI. Facebook has AI teams working on developing the philosophical, as well as technical, foundations for this work. Facebook is also one of the co-founders and members of the Partnership on AI (PAI), a collaborative and multi-stakeholder organization established to study and formulate best practices on AI technologies, to advance the public's understanding of AI, and to serve as an open platform for discussion and engagement about AI and its influences on people and society. The thematic pillars that structure the work we're doing in the scope of the PAI—safety, fairness, transparency and accountability—are the principles that we believe industry should follow and promote when building and deploying AI systems. The PAI's Fair, Transparent and Accountable AI Working Group is also working alongside industry, academia, and civil society to develop best practices around the development and fielding of fair, explainable, and accountable AI systems.

We believe that over the long term, building AI tools is the scalable way to identify and root out most content that violates our policies. We are making substantial investments in building and improving these tools. We already use artificial intelligence to help us identify threats of real world harm from terrorists and others. For example, the use of AI and other automation to stop the spread of terrorist content is showing promise. Today, 99 percent of the ISIS and Al Qaeda related terror content we remove from Facebook is content we detect before anyone in our community has flagged it to us, and in some cases, before it goes live on the site. We do this primarily through the use of automated systems like photo and video matching and text-based machine learning. We also use AI to help find child exploitation images, hate speech, discriminatory ads, and other prohibited content.

I want you to elaborate on what the Europeans got right and what they got wrong.

The GDPR is founded on core principles of accountability, transparency, and control, which are also central values we employ in designing our products. The controls and settings that Facebook is promoting as part of GDPR are available to people around the world, including settings controlling our ability to use data we collect off Facebook Company Products to target ads. We provide the same tools for access, rectification, erasure, data portability and others to people in the US and the rest of the world that we provide in Europe, and many of those tools (like our Download Your Information tool, ad preferences, and Activity Log) have been available globally for many years.

We support the GDPR's emphasis on transparency, choice and control, and its recognition that, while a consent requirement is appropriate in some cases (such as the

processing of sensitive data), other legal frameworks may be appropriate in other circumstances, such as where a company has a "legitimate interest" in processing data, where processing data is necessary to perform a contract, or where data processing serves the broader public interest.

In this way, the GDPR provides strong protections for data that may be processed for different reasons and avoids over-burdening consumers with consent requests for every processing of data, which could increase what experts call "notice fatigue" and cause people to pay less attention to the privacy notices they receive.

On the other hand, GDPR has prescriptive requirements for consent that could require detailed information and an affirmative action from people in ways that may not take into account the context in which people are interacting with an organization. We support models for consent that ensure companies are able to design consent experiences that are intuitive and enhance people's ability to make an informed choice.

Facebook is generally open to the idea of breach notification requirements, particularly legislation that would centralize reporting and ensure a consistent approach across the United States. For example, the GDPR requires notification to a lead supervisory authority, rather than individual member states, in cases of a cross-border data breach. In the United States, however, there is no centralized notification scheme, and instead, reporting obligations vary widely across all 50 states. This complexity makes it harder to respond appropriately and swiftly to protect people in the event of a data breach. We believe this is an important issue and an area that is ripe for thoughtful regulation.

Rep. Rush

When Facebook removed the ability for advertisers to target housing ads based on race.

Discriminatory advertising has no place on Facebook's platform and Facebook removes such content as soon as it becomes aware of it. Facebook's policies prohibit advertisers from discriminating against people on personal attributes such as race, ethnicity, color, national origin, religion, age, sex, sexual orientation, gender identity, family status, disability, and medical or genetic conditions. Facebook educates advertisers on our anti-discrimination policy, and in some cases, requires the advertisers to certify compliance with Facebook's anti-discrimination policy and anti-discrimination laws.

Facebook also uses machine learning to help identify ads that offer housing, employment, or credit opportunities. When an advertiser attempts to show an ad that Facebook identifies as offering a housing, employment, or credit opportunity and includes Facebook's multicultural advertising segments, Facebook will disapprove the ad. Facebook also requires advertisers to certify that they are complying with Facebook's updated anti-discrimination policy and anti-discrimination laws when the advertiser attempts to show a housing, employment, or credit opportunity and uses any other audience segment on Facebook.

Rep. Scalise

You mentioned the Diamond and Silk example where you I think described it as mistake where the people who made that mistake held accountable in any way?

We mishandled communication with Diamond and Silk for months. Their frustration was understandable, and we apologized to them. The message they received on April 5, 2018 that characterized their Page as "dangerous" was incorrect and not reflective of the way we seek to communicate with our community and the people who run Pages on our platform.

As part of our commitment to continually improve our products and to minimize risks where human judgment is involved, we are making a number of changes:

- We have engaged an outside advisor, former Senator Jon Kyl, to advise the company on potential bias against conservative voices. We believe this external feedback will help us improve over time and ensure we can most effectively serve our diverse community.

- We continue to expand our list of outside organizations from across the political spectrum to provide feedback on potential changes to our content standards.

- We have made our detailed reviewer guidelines public to help people understand how and why we make decisions about the content that is and is not allowed on Facebook.

- We have launched an appeals process to enable people to contest content decisions with which they disagree. We recognize that we make enforcement errors on both sides of the equation—what to allow, and what to remove—and that our mistakes cause a great deal of concern for people, which is why we need to allow the option to request review of the decision and provide additional context that will help our team see the fuller picture as they review the post again. This type of feedback will allow us to continue improving our systems and processes so we can prevent similar mistakes in the future.

A study that was done dealing with the algorithm that Facebook uses to describe what is fed to people through the news feed and what they found was after this new algorithm was implemented that there was a tremendous bias against conservative news and content and a favorable bias towards liberal content and if you can look at that, that shows a 16 point disparity, which is concerning. And I know we're almost out of time so if you can go back and look and determine if there was a bias, whoever developed that software, you have 20,000 people that work on some of this data analysis, if you can look and see if there is a bias and let us know if there is and what you're doing about it because that is disturbing when you see that kind of disparity.

Being a platform for all ideas is a foundational principle of Facebook. We are committed to ensuring there is no bias in the work we do.

Suppressing content on the basis of political viewpoint or preventing people from seeing what matters most to them is directly contrary to Facebook's mission and our business objectives.

When allegations of political bias surfaced in relation to Facebook's Trending Topics feature, we immediately launched an investigation to determine if anyone violated the integrity of the feature or acted in ways that are inconsistent with Facebook's policies and mission. We spoke with current reviewers and their supervisors, as well as a cross-section of former reviewers; spoke with our contractor; reviewed our guidelines, training, and practices; examined the effectiveness of operational oversight designed to identify and correct mistakes and abuse; and analyzed data on the implementation of our guidelines by reviewers.

Ultimately, our investigation revealed no evidence of systematic political bias in the selection or prominence of stories included in the Trending Topics feature. In fact, our analysis indicated that the rates of approval of conservative and liberal topics are virtually identical in Trending Topics. Moreover, we were unable to substantiate any of the specific allegations of politically-motivated suppression of subjects or sources, as reported in the media. To the contrary, we confirmed that most of those subjects were in fact included as trending topics on multiple occasions, on dates and at intervals that would be expected given the volume of discussion around those topics on those dates.

Nonetheless, as part of our commitment to continually improve our products and to minimize risks where human judgment is involved, we are making a number of changes:

- We have engaged an outside advisor, former Senator Jon Kyl, to advise the company on potential bias against conservative voices. We believe this external feedback will help us improve over time and ensure we can most effectively serve our diverse community and build trust in Facebook as a platform for all ideas.

- We continue to expand our list of outside partner organizations to ensure we receive feedback on our content policies from a diverse set of viewpoints.

- We have made our detailed reviewer guidelines public to help people understand how and why we make decisions about the content that is and is not allowed on Facebook.

- We have launched an appeals process to enable people to contest content decisions with which they disagree.

- We are instituting additional controls and oversight around the review team, including robust escalation procedures and updated reviewer training materials.

These improvements and safeguards are designed to ensure that Facebook remains a platform for all ideas and enables the broadest spectrum of free expression possible.

With respect to News Feed, a user's News Feed is made up of stories from their friends, Pages they've chosen to follow, and groups they've joined. Ranking is the process we use to organize all of those stories so that users can see the most relevant content at the top, every time

they open Facebook. Ranking has four elements: the available inventory of stories; the signals, or data points that can inform ranking decisions; the predictions we make, including how likely we think a user is to comment on a story, share with a friend, etc.; and a relevancy score for each story.

News Feed considers thousands of signals to surface the content that's most relevant to each person who uses Facebook. Our employees don't determine the ranking of any specific piece of content. To help the community understand how News Feed works and how changes to News Feed affect their experience on Facebook, we publish a regularly-updated News Feed FYI blog (https://newsroom.fb.com/news/category/inside-feed/) where our team shares details of significant changes.

Is that data that is mined for security purposes after a user logs off also used to sell as part of the business model?

When people visit apps or websites that feature our technologies—like the Facebook Like or Comment button—our servers automatically log (i) standard browser or app records of the fact that a particular device or user visited the website or app (this connection to Facebook's servers occurs automatically when a person visits a website or app that contains our technologies, such as a Like button, and is an inherent function of internet design); and (ii) any additional information the publisher of the app or website chooses to share with Facebook about the person's activities on that site (such as the fact that a purchase was made on the site). This is a standard feature of the internet, and most websites and apps share this same information with multiple different third-parties whenever people visit their website or app. For example, the House Energy and Commerce Committee's website shares information with Google Analytics to help improve the site. This means that, when a person visits the Committee's website, it sends browser information about their visit that third party. More information about how this works is available at https://newsroom.fb.com/news/2018/04/data-off-facebook/.

When the person visiting a website featuring Facebook's tools is not a registered Facebook user, Facebook does not have information identifying that individual, and it does not create profiles for this individual.

We use the browser and app logs that apps and websites send to us—described above—in the following ways for non-Facebook users. First, these logs are critical to protecting the security of Facebook and to detecting or preventing fake account access. For example, if a browser has visited hundreds of sites in the last five minutes, that's a sign the device might be a bot, which would be an important signal of a potentially inauthentic account if that browser then attempted to register for an account. Second, we aggregate those logs to provide summaries and insights to websites and apps about how many people visit or use their product, or use specific features like our Like button—but without providing any information about a specific person. We do not create profiles for non-Facebook users, nor do we use browser and app logs for non-Facebook users to show targeted ads from our advertisers to them or otherwise seek to personalize the content they see. However, we may take the opportunity to show a general ad that is unrelated to the attributes of the person or an ad encouraging the non-user to sign up for Facebook.

When the individual is a Facebook user, we are also able to use this information to personalize their experiences on Facebook, whether or not they are logged out, but we will not target ads to users relying on this information unless the user allows this in their privacy settings. We do not sell or share this information with third-parties.

We do receive some information from devices and browsers that may be used by non-users. For example:

- We also may receive information about the device of a non-registered user if that user visits a part of Facebook that does not require people to log in—such as a public Facebook Page. The information we log when people visit our websites or apps is the same as described above and is the same information that any provider of an online service would receive.

- In addition, Facebook may receive some basic information about devices where Facebook apps are installed, including before people using those devices have registered for Facebook (such as when a user downloads a Facebook app, but has not yet created an account, or if the app is preloaded on a given device). This device data includes things like device model, operating system, IP address, app version and device identifiers. We use this information to provide the right version of the app, help people who want to create accounts (for example, optimizing the registration flow for the specific device), retrieving bug fixes and measuring and improving app performance. We do not use this information to build profiles about non-registered users.

Rep. Schakowsky

Kogan also sold data to other firms. You named Eunoia Technologies. How many are there total and what are their names? Can we get that and how many are there total?

Kogan represented that, in addition to providing data to his Prosociality and Well-Being Laboratory at the University of Cambridge for the purposes of research, GSR provided some Facebook data to SCL Elections Ltd., Eunoia Technologies, and the Toronto Laboratory for Social Neuroscience at the University of Toronto. However, the only party Kogan has claimed paid GSR was SCL. Our investigation is ongoing.

Rep. Upton

Why an ad for a state senate candidate in Michigan, which said "be a pro-life, pro-2nd Amendment lawmaker," was taken down.

We acknowledge that an ad announcing the candidacy of Aric Nesbitt in Michigan was improperly rejected. The rejection was the result of an automated systems error, which caused thousands of other ads—including an ad for a progressive news article—to be improperly rejected. The ad at issue should not have been rejected and was reapproved within hours, as soon as we discovered the systems error. Every advertiser affected by this error was sent an email letting them know their ads had been approved. The automated rule that resulted in the ad disapprovals was turned off.

Rep. Walden

I want to flag an issue that Vietnam Veterans of America have raised.

We recently released enforcement statistics in our Community Standards Enforcement Report, including how many Facebook accounts we took action on because we determined they were fake. We will refine our approach over time, and we also hope to release additional metrics in future reports.

I would welcome your suggestions of other technology CEOs we might benefit from hearing from in the future for hearing on these issues as we look at net neutrality, and privacy issues, these are all important. They are very controversial. We are fully cognizant of that.

We would suggest speaking with one of the many trade associations that represent the technology industry. These associations are uniquely positioned to provide insights on trends, technologies, policies and related issues that affect their members and to discuss trends across companies in our industry. They are an excellent resource for governments as they seek to promote innovation and economic growth for the benefit of all stakeholders in the digital economy.

Given the situation, can you manage the issues that are before you or does Congress need to intercede? I'm going to leave that because I'm over my time.

Facebook is generally not opposed to regulation but wants to ensure it is the right regulation. We are already regulated in many ways—for example, under the Federal Trade Commission Act—and we are subject to ongoing oversight by the FTC under the terms of a 2011 Consent Order. Facebook has inherent incentives to protect its customers' privacy and address breaches and vulnerabilities. Indeed, the recent discovery of misconduct by an app developer on the Facebook platform clearly hurt Facebook and made it harder for us to achieve our social mission. As such, Facebook is committed to protecting our platform from bad actors, ensuring we are able to continue our mission of giving people a voice and bringing them closer together. We are also actively building new technologies to help prevent abuse on our platform, including advanced AI tools to monitor and remove fake accounts. We have also significantly increased our investment in security, employing more than 15,000 individuals working solely on security and content review and planning to increase that number to over 20,000 by the end of the year. We have also strengthened our advertising policies, seeking to prevent discrimination while improving transparency.

Rep. Welch

Do you believe that consumers should be able to correct or delete inaccurate personal data that companies have obtained?

As explained in our Data Policy, we collect three basic categories of data about people: (1) data about things people do and share (and who they connect with) on our services; (2) data about the devices people use to access our services; and (3) data we receive from partners, including the websites and apps that use our business tools. Our Data Policy provides more detail about each of the three categories.

We use this information for a variety of purposes, including to provide, personalize, and improve our products; provide measurement, analytics, and other business services; promote safety and security; to communicate with people who use our services; and to research and innovate to promote the social good. We provide more information in our Data Policy about these uses as well.

Our policies limit our retention of the data that we receive in several ways. Specifically, we store data until it is no longer necessary to provide our services and Facebook products, or until a person's account is deleted—whichever comes first. This is a case-by-case determination that depends on things like the nature of the data, why it is collected and processed, and relevant legal or operational retention needs. If a user posts something on their Facebook profile, then that information would be retained until they delete it or until they delete their account.

We also have other policies that are designed to limit our retention of other types of information about people. For example, if a user clicks a "Like" button that appears on a third-party site, we may use that information to show the person a more personalized experience on Facebook, to help maintain and improve our service, and to protect both the user and Facebook from malicious activity. We delete or anonymize the URL where the Like occurred within 90 days.

In general, when a user deletes their account, we delete things they have posted, such as their photos and status updates, and they won't be able to recover that information later. (Information that others have shared about them isn't part of their account and won't be deleted.)

There are some limited exceptions to these policies: For instance, information can be accessed and preserved for an extended period when it is the subject of a legal request or obligation, governmental investigation, or investigations of possible violations of our terms or policies, or otherwise to prevent harm. We also retain information from accounts disabled for terms violations for at least a year to prevent repeat abuse or other term violations.

Particularly in the past few months, we've realized that we need to take a broader view of our responsibility to our community. Part of that effort is continuing our ongoing efforts to identify ways that we can improve our privacy practices. This includes restricting the way that developers can get information from Facebook and announcing plans to build Clear History, a new feature that will enable users to see the websites and apps that send us information when they use them, clear this information from their accounts, and turn off our ability to store it associated with their accounts going forward.

Rep. Eshoo

Are you willing to change your business model in the interest of protecting individual privacy?

Like many other free online services, we sell advertising space to third parties. Doing so enables us to offer our services to consumers for free. This is part of our mission to give people the power to build community and bring the world closer together.

As explained in our Data Policy, we collect three basic categories of data about people: (1) data about things people do and share (and who they connect with) on our services, (2) data about the devices people use to access our services, and (3) data we receive from partners, including the websites and apps that use our business tools. Our Data Policy provides more detail about each of the three categories.

We use this information for a variety of purposes, including to provide, personalize, and improve our products, provide measurement, analytics, and other business services, promote safety and security, to communicate with people who use our services, and to research and innovate to promote the social good. We provide more information in our Data Policy about these uses as well.

Our policies limit our retention of the data that we receive in several ways. Specifically, we store data until it is no longer necessary to provide our services and Facebook products, or until a person's account is deleted—whichever comes first. This is a case-by-case determination that depends on things like the nature of the data, why it is collected and processed, and relevant legal or operational retention needs. For example, if a user posts something on their Facebook profile, then that information would be retained until they delete it or until they delete their account.

In general, when a user deletes their account, we delete things they have posted, such as their photos and status updates, and they won't be able to recover that information later. (Information that others have shared about them isn't part of their account and won't be deleted.) There are some limited exceptions to these policies: For instance, information can be accessed and preserved for an extended period when it is the subject of a legal request or obligation, governmental investigation, or investigations of possible violations of our terms or policies, or otherwise to prevent harm. We also retain information from accounts disabled for terms violations for at least a year to prevent repeat abuse or other term violations.

In our ongoing efforts to identify ways that we can improve our privacy practices, we're building new experiences to help people understand how we collect and use data. This includes further restricting the data third-party app developers can ask people to share and announcing plans to build Clear History, a new feature that will enable users to see the websites and apps that send us information when they use them, clear this information from their accounts, and turn off our ability to store it associated with their accounts going forward.

Rep. Ruiz

I look forward to working with you and the committee to better protect consumer privacy.

Facebook is generally not opposed to regulation but wants to ensure it is the right regulation. The issues facing the industry are complex, multi-faceted, and affect an important part of peoples' lives. As such, Facebook is absolutely committed to working with regulators, like Congress, to craft the right regulations. Facebook would be happy to review any proposed legislation and provide comments.