NEAL R. GROSS & CO., INC.
RPTS MASSIMO
HIF333160

ALGORITHMS: HOW COMPANIES' DECISIONS ABOUT
DATA AND CONTENT IMPACT CONSUMERS
WEDNESDAY, NOVEMBER 29, 2017
House of Representatives
Subcommittee on Communications and
Technology
joint with the
Subcommittee on Digital Commerce and Consumer
Protection
Committee on Energy and Commerce
Washington, D.C.

The subcommittee met, pursuant to call, at 10:00 a.m., in Room 2123 Rayburn House Office Building, Hon. Robert Latta [chairman of the Subcommittee on Digital Commerce and Consumer Protection] presiding.

Present from the Subcommittee on Digital Commerce and Consumer Protection: Representatives Latta, Harper, Burgess, Lance, Guthrie, Kinzinger, Bilirakis, Bucshon, Mullin, Walters, Costello, Walden (ex officio), Schakowsky, Clarke, Dingell, Matsui, Welch, Green, and Pallone (ex officio).

Present from the Subcommittee on Communications and Technology: Representatives Blackburn, Lance, Shimkus, Latta, Guthrie, Olson, Kinzinger, Bilirakis, Johnson, Flores, Brooks, Collins, Cramer, Walters, Costello, Walden (ex officio), Doyle, Welch, Clarke, Loebsack, Ruiz, Dingell, Eshoo, Engel, Matsui, McNerney, and Pallone (ex officio).

Staff present: Mike Bloomquist, Deputy Staff Director; Samantha Bopp, Staff Assistant; Kelly Collins, Staff Assistant; Robin Colwell, Chief Counsel, Communications and Technology; Sean Farrell, Professional Staff Member, Communications and Technology; Margaret Tucker Fogarty, Staff Assistant; Melissa Froelich, Chief Counsel, Digital Commerce and Consumer Protection; Adam Fromm, Director of Outreach and Coalitions; Gene Fullano, Detailee, Communications and Technology; Ali Fulling, Legislative Clerk, Oversight and Investigations, Digital Commerce and Consumer Protection; Theresa Gambo, Human Resources/Office Administrator; Elena Hernandez, Press Secretary; Paul Jackson, Professional Staff, Digital Commerce and Consumer Protection; Bijan Koohmaraie, Counsel, Digital Commerce and Consumer Protection; Tim Kurth, Senior Professional Staff, Communications and Technology; Lauren McCarty, Counsel, Communications and Technology; Katie McKeogh, Press Assistant;

Alex Miller, Video Production Aide and Press Assistant; Mark Ratner, Policy Coordinator; Madeline Vey, Policy Coordinator, Digital Commerce and Consumer Protection; Evan Viau, Legislative Clerk, Communications and Technology; Hamlin Wade, Special Advisor, External Affairs; Everett Winnick, Director of Information Technology; Greg Zerzan, Counsel, Digital Commerce and Consumer Protection; Michelle Ash, Minority Chief Counsel, Digital Commerce and Consumer Protection; Jeff Carroll, Minority Staff Director; David Goldman, Minority Chief Counsel, Communications and Technology; Lisa Goldman, Minority Counsel; Lori Maarbjerg, Minority FCC Detailee; Dan Miller, Minority Policy Analyst; Caroline Paris-Behr, Minority Policy Analyst; and C.J. Young, Minority Press Secretary.

Mr. Latta. Well, good morning. I would like to call our joint subcommittee meeting to order and the chair recognizes himself for 5 minutes for an opening statement.

And good morning again. I would like to welcome everyone back from Thanksgiving holiday to our joint subcommittee hearing. I would like to thank our witnesses for being here today. I would venture to guess many people were able to get a jumpstart on their holiday shopping and seeing some of the earlier reports showing that online shopping rose 17 percent from last year which makes our hearing this morning even more timely.

When Chairman Walden became chairman of the Energy and Commerce Committee we agreed that keeping our focus on the consumer was a priority for the committee. And everything that the Digital Commerce and Consumer Protection Subcommittee has done, whether it has been exploring new technologies through our Disrupter Series or the bipartisan work that went into the SELF DRIVE Act, our goal has always been to act in the best interest of the consumer, the American people.

Earlier this fall, the Equifax data breach compromised the personal information of over 145 million Americans. This troubling incident raised many questions about credit industry practices with respect to the collection of consumer information. Many Americans, some of whom never heard of Equifax, were confused as to how their sensitive personal information could have been compromised by a company they had never interacted with.

Just last week, Uber announced their systems were hacked, exposing data of over 57 million users. Rather than alert authorities and make the breach known to their users and drivers, Uber kept the hack secret for a year. Disregard of law and disregard of consumers' and drivers' trust all require close scrutiny. The Digital Commerce and Consumer Protection Subcommittee will continue our work to protect consumers and make sure those who disregard the law are held accountable.

As investigations continue, the importance of this hearing cannot be understated. Polls show Americans both feel that technology has had a positive effect on our society, but are also skeptical about how their information is used by major technology companies. As policymakers, it is our obligation to ask the tough questions and make sure consumers understand how their information is being used in our digitally-driven economy.

That is why we explore today how personal information about consumers is collected online and, importantly, how companies use that information to make decisions about the content consumers see. Right now, there are more than 224 million smart phone users in America and U.S. consumers spend about 5 hours a day on their mobile devices. As we continue to see the number of connected devices increase and our digital economy expand, Americans are only going to spend more and more time online browsing the web, shopping, or checking social media with more information about them being collected.

Although there are legitimate reasons and benefits of the collection and use of information online, we want to ensure that Americans understand how their information is being used. Specifically, how do companies use algorithms to make decisions and deliver content to consumers? What information goes into these complex algorithms and how do they control the information that comes out? How important are human decisions in creating the algorithms and interpreting the results? Are the results of the researches we conduct online objective or are companies controlling the information we get?

These are all fair, legitimate questions that we intend to explore. It is our job to make sure consumers have the information they need to make informed decisions, especially when it comes to the flow of their personal information online. With that said, it is also important to understand how effective privacy policy disclosures are. Although some scholars believe such disclosures empower the consumers, others contend they are only there for the lawyers and are impossible to read. For that reason, we must consider whether there are more effective ways to empower the consumer.

I would like to thank Chairman Blackburn for her commitment to these issues and I look forward to exploring these complex but important issues with all stakeholders. Again I want to thank our witnesses for being here today and at this time I would like to recognize the gentlelady from Illinois, the ranking member of the subcommittee, for 5 minutes.

Ms. Schakowsky. Thank you, Mr. Chairman. We like to think of the internet as an open marketplace and forum for the exchange of ideas. In reality, the information that consumers see is determined in part by tech companies. Today, algorithms determine what appears in web ads, search results, and your customized news feed. Some of the content you are presented may be based on personal information such as your gender, race, and location. It may also depend on how much companies have paid to get that content in front of you.

The internet and social media have changed how Americans consume news, information, and advertising. According to an August 2017 survey by the Pew Research Center, two-thirds of Americans get at least some of their news through social media. Consumers rely on a handful of popular platforms, making the algorithms of those platforms tremendously powerful.

On a sinister level, organizations and even nation-states can exploit algorithms to spread disinformation as we saw with Russian interference in the 2016 elections. In addition, platforms profit by selling ads targeted to specific groups based on their demographics and inferences made through their engagement with content on the platform. This may have some benefit, consumers see ads that they are actually interested in, but the line between tailoring advertising and facilitating discrimination can get murky. As we grapple with algorithms on the internet, the Federal Communications Commission is considering big changes that would allow corporations to further shape what content consumers access. On December 14th, the FCC will vote on whether to undo the Open Internet Order which protects net neutrality. If that proposal is adopted, internet service providers will be able to control consumers' access to content. They can make website load faster or slower depending on whether the content provider pays for the better speed, or an ISP can block content altogether.

Destroying that neutrality would change the internet as we know it, and how does a small business compete online if it now has to pay every ISP in the country for its website to load as fast as a big corporation competitors? What happens to the exchange of ideas when access to some content is restricted? This is a disturbing amount of power that the FCC might cede to for-profit broadband providers.

We already have examples of what broadband providers do when empowered to block content. Verizon blocked text messages from reproductive rights group NARAL calling them, quote, controversial, unquote. AT&T limited use of Face Time to incentivize its customers to purchase more expensive data plans. TELUS, another telecom company, blocked the website of a union with which it had a labor dispute. No wonder millions of internet users have filed comments in support of maintaining the Open Internet Order. Just since last Monday, my office has received about 500 calls from net neutrality supporters.

Americans are watching the FCC's next move. The FCC under Chairman Pai is also encouraging consolidation and media ownership. It has bent over backward to clear the way for Sinclair Broadcast Group's acquisition of Tribune Media. Congress established a 39 percent cap on the national audience one broadcaster can cover, but Chairman Pai moved to reinstate the outdated UHF discount so that Sinclair can potentially cover 70 percent of the national audience. This media consolidation is a threat to local journalism, especially as Sinclair forces its stations to run nationally produced, quote, must-air, unquote, content.

Big corporations are being given more and more influence over the information that Americans receive from news feeds to websites, from smart phone to TVs. Congress and federal watchdogs like the FCC have a responsibility to push back on corporate power when it threatens fair competition and free expression. I look forward to our witnesses' insights on how we fulfill that responsibility and I yield back. Thank you.

Mr. Latta. Thank you. The gentlelady yields back and this time the chair recognizes the gentlelady from Tennessee, the chairman of the Communications and Technology Subcommittee, for 5 minutes.

Mrs. Blackburn. Good morning and welcome to all of our witnesses. I want to thank my colleague Mr. Latta for working closely with me and our committee to put together this stellar panel so that we can talk about all things virtual.

Although we often refer to the world on the other side of the screen as the virtual world, we are seeing that when things go wrong the real-world impacts on our privacy, finances, knowledge base, and even freedom of expression are anything but virtual. They are very, very real. As so many of these issues overlap between our two subcommittees, I am pleased we are able to kick off our exploration of these issues as a team.

On a number of fronts we are seeing the pressure turned up on the tech companies that often serve as the new town squares for public discourse as governments and users are demanding that certain speech be shut down. Some of the responses have perhaps been a disappointment from the perspective of free speech. Companies that began as start-ups in Silicon Valley garages have fundamentally changed the way we communicate with one another about everything from the song we want to hear to what stock to buy to what is the best way to change our healthcare delivery system.

These multinational corporations now respond to pressures that do not necessarily align with American values, so we need to examine how and why content is being blocked, filtered, or prioritized. This may all sound faintly similar to another topic, net neutrality. Exercise caution here as it is important to note the FCC's current rules only apply to ISPs, not social media or search platforms.

In some very concrete ways, the open internet is being threatened by certain content management practices. These 2 year old FCC rules have not and cannot address these threats, do it is disheartening to see Title II regulatory advocates happily conflating the two to divert attention from who is actually blocking content. The current FCC proposal to return internet regulation back to the bipartisan light touch norm also reminds us that we are simply shifting authority back to the FTC to handle privacy matters.

The previous head of the FCC swiped jurisdiction from the FTC, a 100-plus year old institution established by a Democratic President to act against trust. As discussed at our previous hearings on the limits of the FCC, its authority can only touch one part of the internet ecosystem and thus it ignores edge provider services that collect arguably more data than ISPs.

As you may have heard, in order for consumers to be able to protect their virtual you, I introduced a bill that would create a level and fair privacy playing field by bringing all entities that collect and sell personal data of individuals under the same unified rules. Given the witnesses' testimony today, let me also plug another bipartisan initiative we have addressed, data security. Given the implications and risk associated with transferring all of this data, it is imperative that we address data security. It is a timely issue.

I look forward to working with my friends across the aisle on this, data security and on privacy, the BROWSER Act, and all of these topics so that we can settle our differences right here with legislative authority in these hearing rooms rather than relinquishing that authority to regulators in power. I thank the chairman for his collaboration and work on this issue and I yield back the balance of my time.

Mr. Latta. Thank you. The gentlelady yields back. And before I recognize our next member I just want to mention to our witnesses we have another subcommittee that is going on right now so you will have members coming in and out of subcommittee today. And at this time the chair recognizes the gentleman from Pennsylvania, the ranking member on C and T, for 5 minutes.

Mr. Doyle. Thank you, Mr. Chairman, for holding this joint hearing and thank you to the witnesses who have come before us today.

Machine learning and artificial intelligence are powerful tools that are reshaping our country and our economy. In places like my hometown of Pittsburgh, our leadership in artificial intelligence is leading to new technologies and new advances that have the potential for revolutionary changes. I hope this committee can continue to investigate and understand this important technology and the impacts that it will have.

That being said, troubling recent events such as the hack of Equifax continue to show light on the dark world of data brokers and data mining. Credit rating agencies play a central role in many Americans' lives whether you are buying a home, a car, or even a new phone. Your ability to demonstrate good credit in the eyes of these institutions is tantamount to being allowed to make a purchase or being told that you do not pass go. Americans have little recourse and our government provides little oversight of these institutions and their practices. They are increasingly using big data and machine learning to make judgments about individuals and their ability to access and use credit.

Data breaches at these companies pose grave threats to nearly every American and I think this warrants further investigation. However, today I am deeply concerned that this hearing is happening in the shadow of the FCC's efforts to end network neutrality and this Congress's own decision to use the Congressional Review Act on the FCC's broadband privacy rules. These policies are and were robust protections for consumers that are at the heart of our discussions here today.

In addition, Ms. Moy's testimony refers in numerous places to the CRA against rules requiring mandatory arbitration by financial institutions. The majority does not seem content to merely strip Americans of their legal and regulatory protections. They are going even further now and working to deny them their access to the courts as well. The majority seems willing only to give lip-service to these real consumer protections that they have already cast aside.

The FCC's current efforts to repeal the Open Internet Order and end network neutrality are a perfect case in point. The need for net neutrality was borne out of a long history of anti-consumer and anti-competitive behavior that limited consumers' access to content and information, new technologies, and competitive choices. ISPs have blocked consumer access to services that compete with their own services, new services, and transformative services more times than I can count. The FCC's privacy rules themselves were a reaction to bad behavior by the ISPs.

For years, ISPs have taken actions to track user behavior online using deep packet inspection, undeletable supercookies, and even force consumers to pay them on top of the sky-high fees they already charge to retain their privacy. Consumers were protected from these abusive practices until Congress and President Trump recklessly acted to nullify these rules.

I cannot reiterate to my colleagues enough that when you own the pipe to the home you own access to the consumer as ISPs have demonstrated so many times. Repealing these rules will have grave consequences on consumers and the vibrance of the online ecosystem. I continue to urge Chairman Pai to end his quixotic misadventure, and with that being said I will yield the remainder of my time to Mr. McNerney.

Mr. McNerney. I thank the ranking member. While I am glad we are holding today's hearing about protecting online consumers, I am disappointed that the Republicans on this committee and at the Federal Communications Commission are doing just the opposite. Earlier this year, Republicans passed the privacy CRA eliminating broadband privacy protections for consumers' personal information.

In response, I introduced the MY DATA Act. This legislation would give the Federal Trade Commission rulemaking and enforcement authority so that consumers can have strong privacy and data security protections across the internet. Not a single Republican agreed to cosponsor this bill. In addition, this December, the FCC is expected to adopt Chairman Pai's proposal to dismantle net neutrality. Thousands of constituents have reached out to my office this year to express concerns about eliminating broadband privacy and net neutrality protections. I urge my Republican colleagues to take actions to actually protect consumers instead of talking about protecting consumers while exposing consumers to online mischief. I yield back.

Mr. Latta. Thank you very much. The gentleman yields back. And at this time, the chair now recognizes the gentleman from Oregon, the chairman of the full committee, for 5 minutes.

The Chairman. Thank you, Mr. Latta, and good morning, everyone. Thanks for being here, especially thanks to our witnesses.

And today we begin a critical discussion about the evolution of consumers' online environment. We will dive into many of the important questions surrounding the future of data access and content management in a marketplace driven by algorithms. Just in the past decade, the internet economy has grown, thrived, and evolved, as you all know, substantially. It is amazing what is happening there.

The smart phones we carry with us everywhere, the tablets we log on to, the smart home devices in our kitchens, all represent a transformational shift in how Americans gather information, receive their news and content, and how they connect with friends and with family. These services are convenient, efficient, and provide valuable and tangible benefits to American consumers.

The companies behind the services have created thousands and thousands of jobs and brought the U.S. into the forefront of technology and innovation. In exchange for using certain websites or platforms, consumers are willing to share personal details about themselves -- names, locations, interests, and more. The context of the relationship drives that exchange.

Now depending on the service, tech companies and online platforms make their money because they know who you are, where you are, what you like, what photos and videos you take and watch, and what news you read. The depth and power of data will be supercharged with the proliferation of connected and embedded devices in the Internet of Things. Billions of IoT devices will surely be deployed linking machines to other machines and transmitting massive amounts of data and information to connect Americans to even more services, conveniences, and benefits from all around the globe.

So what is behind these services and activities? Algorithms and data. Algorithms are a sequence of instructions to solve a problem or complete a task. These instructions help devices and apps predict user preferences as well as provide the content and advertising you see in your social media feed. Data serve as inputs or signals to those algorithms. Well-intentioned algorithms can lead to unanticipated consequences. For example, algorithmic bots are being profusely designed to steal or to cheat in online gambling and ticket sales.

Humans remain a critical part of the creation and monitoring of these systems. In recent months, reports of data breaches and algorithms gone awry have demonstrated the potentially negative influences of digital technology on Americans' lives. This committee has done extensive work on issues surrounding consumer protection and data breaches. We brought in the former CEO of Equifax for a hearing and we continue to push for answers on behalf of American consumers. At the same time, there have been some high profile instances of major social media platforms blocking content for questionable reasons using opaque processes. As a result of all of this, consumers are concerned about whether they can trust online firms with the integrity of news and information they disseminate, the welfare of its users, and on a much larger scale the preservation of our own democratic institutions. All these are part of the big public discussion going on right now.

As we all know net neutrality is the issue of the moment, but regardless of where you stand on that policy the recent attacks on Chairman Pai and particularly his children are completely unacceptable and have no place in this debate. Period. I condemn it in the strongest terms and I call on the entire tech community and my colleagues on both sides of the aisle to condemn it as well.

In light of the current controversy surrounding net neutrality rules for ISPs, it is important to examine how content is actually being blocked or promoted or throttled every day on the internet and not by the ISPs. Net neutrality rules do not address the threats to the open internet that we will discuss today.

Now the goal for today's hearing is to help provide all Americans with a better understanding of how their data flows online, how online platforms and online media sources determine what they see or don't see, and the extent of and methods by which their information is collected and used by online firms. Americans should be able to feel confident that their well-being, freedom of expression, and access to the content of their choice are not being wholly sacrificed for profit.

Americans should have vibrant, competitive markets both offline and online where consumers know their rights and options and have the freedom to choose what is best for their circumstances. It is undeniable the internet has created millions of new jobs, tremendous opportunities, access in ways unimaginable just a few years ago, but it has also created these new risks and challenges.

So in the name of convenience is there a potential for online firms to undermine America's privacy and security in a way that they don't expect or know about? Are the current policies regarding the collection and use of personal data working? Are consumers harmed by this hyperpersonalization? And finally, are firms' content management practices constraining America's ability to speak and to listen freely on an open internet?

Consumers should remain as safe from unfair, deceptive, and malicious practices by online firms and their algorithms on the internet as they do in the real world. And we are here today to dig into these tough questions and we appreciate your advice and counsel from our witnesses today. And with that Mr. Chair I yield back.

Mr. Latta. Thank you very much. The gentleman yields back and at this time the chair recognizes the gentleman from New Jersey, the ranking member of the full committee, for 5 minutes.

Mr. Pallone. Thank you, Mr. Chairman. The internet is home to some of the most important conversations taking place today. As internet companies find ways for Americans to communicate our democracy should be stronger than ever, but as you all know something else is going on. Our national dialogue is being curated by companies policing content and the number of websites handling this traffic has consolidated to just a few key players.

The aim of internet platforms is monetizing web traffic, not public policy. Algorithms created for the purpose of increasing ad clicks is what ends up shaping what we see online and too often this content is not an accurate reflection of the real world. Structural flaws built into the algorithms used to sort online content may result in racial and other bias in our news feeds.

As diverse voices are squeezed out, bias increases even further and this is simply not acceptable and I look forward to hearing more today about what we can do about it. Unfortunately, forces are at work here in Washington that make this problem worse. At every turn we see efforts to give more power to gatekeepers either by eviscerating net neutrality and privacy or by picking favorite voices for preferred regulatory treatment.

Even now as we hold a hearing to talk about mitigating bias on the internet, FCC Chairman Pai is planning to introduce more bias into the system. The net neutrality rules that he plans to destroy are the protections that ensure that we the people can decide for ourselves what we do and say online and Chairman Pai's plan will fundamentally change the free and open internet as we know it. Independent voices, those outside the mainstream may be most at risk simply because they don't have an affiliation with the companies that run the internet.

Unfortunately, broadband companies have more than just financial reasons to obstruct access to independent content, it can also be political. Under Chairman Pai's plan, nothing stops those in power from pushing broadband companies to sensor dissenting voices or unpopular opinions or to promote views that they support. We are seeing more and more often how this Administration is using its political might to pressure even large companies.

And this is not a partisan point or even a political one.

Jeopardizing the national dialogue should concern all of us. The dialogue that happens online is critical for our democracy. Chairman Pai's move comes after this Congress acted earlier this year to wipe out privacy and data security online. Under President Obama the FCC adopted fair rules to protect the little guy. Ask before collecting information, don't share it without consent, and take reasonable measures to safeguard it. But that was too much for congressional Republicans who voted to take away these protections and hand over consumers' data to big business.

Sadly, there is still more to come. Over this past year, the FCC has taken every step possible to ensure that Sinclair broadcasting, already the largest owner of broadcast stations in the country becomes even bigger. And these steps by the FCC fly in the face of laws Congress put in place to protect local voices. We understand that diverse perspectives are critical for our communities and strengthen our democracy. Instead, the FCC is doing everything it can to allow one company to control what people hear no matter where they are in the country and that is simply not what we intended.

So I look forward to discussing ways to eliminate bias in our communication systems. We need to figure out how to wrest power over information from corporations and return it back to the people. And I yield the remainder of my time to the gentlewoman from New York, Ms. Clarke.

Ms. Clarke. I thank you, Mr. Ranking Member Pallone, for yielding me time. Today's hearing is of great importance to me for various reasons both as a congresswoman and as a consumer. You see, technology continues to touch all areas of our lives and its reach will continue to grow in the coming days, weeks, months, and years.

With greater reach comes greater responsibility. Companies must ensure that the algorithms used for their services and products are free from all biases including racial, ethnic, gender, sexual orientation biases. That includes making sure there is a diverse employee base behind the scenes ensuring these algorithms accurately represent American consumers.

As a member of the Congressional Black Caucus I would like to highlight the great work of the CBC Diversity Task Force and the CBC TECH 2020 initiative, two entities that have been doing a substantive deep-dive analysis into the progress of the American tech sector in accomplishing meaningful diversity and inclusion in the technology space. Additionally, I would like unanimous consent to submit for the record a letter my colleagues, Representatives Butterfield, Cleaver, and Kelly, and myself, sent to Facebook regarding their site's use of ethnic affinity search criteria which allow users to violate the Fair Housing Act. This is just an example of abuse within the algorithm space that really needs to be monitored and addressed and I hope that we will get some recommendations from you here today.

It is my understanding that this is being addressed in the short term through Facebook. I just want to go on the record that this is a concern to my colleagues and I. These issues are vitally important and I look forward to today's testimony. Mr. Chairman, I yield back.

Mr. Latta. And without objection, the letter is accepted for the record.

[The information follows:]

**********COMMITTEE INSERT 1**********

Mr. Latta. And the gentlelady yields back. This concludes the member opening statements. The chair reminds members that pursuant to the committee rules, all members' opening statements will be made part of the record. Additionally, I ask unanimous consent that Energy and Commerce members not on the Subcommittee on Digital Commerce and Consumer Protection or the Subcommittee on Communications and Technology be permitted to participate in today's hearing. Without objection, so ordered.

Again I want to thank our witnesses for being with us today and because it is very important for us to hear from you and being to testify before the subcommittee. Today's witnesses will have the opportunity to give 5-minute opening statements followed by a round of questions from our members. Our witness panel for today's hearing will include Dr. Omri Ben-Shahar, the Leo and Eileen Herzel Professor of Law at the University Chicago of Law; Ms. Kate Klonick, the Resident Fellow for the Information Society Project at Yale Law School; Ms. Laura Moy, the Deputy Director of the Georgetown Law Center on Privacy and Technology; Dr. Catherine Tucker, the Sloane Distinguished Professor of Management and Science and Professor of Marketing at the MIT Sloane School of Management; Mr. Frank Pasquale, the Professor of Law at the University of Maryland, Francis King Carey School of Law; and Dr. Michael Kearns, the Professor and National Center Chair of the Department of Computer and Information Science at the University of Pennsylvania.

Again I want to thank all of our witnesses for being with us today, and again you each have 5 minutes. If you will, just pull that mike up close and turn on the button. We look forward to hearing your testimony.

And Doctor, we will start with you this morning. Thank you.

STATEMENTS OF OMRI BEN-SHAHAR, LEO AND EILEEN HERZEL PROFESSOR OF LAW, UNIVERSITY OF CHICAGO LAW SCHOOL; KATE KLONICK, RESIDENT FELLOW, INFORMATION SOCIETY PROJECT, YALE LAW SCHOOL; LAURA MOY, DEPUTY DIRECTOR, GEORGETOWN LAW CENTER ON PRIVACY AND TECHNOLOGY; CATHERINE TUCKER, SLOANE DISTINGUISHED PROFESSOR OF MANAGEMENT SCIENCE AND PROFESSOR OF MARKETING, MIT SLOANE SCHOOL OF MANAGEMENT; FRANK PASQUALE, PROFESSOR OF LAW, UNIVERSITY OF MARYLAND; AND, MICHAEL KEARNS, PROFESSOR AND NATIONAL CENTER CHAIR, DEPARTMENT OF COMPUTER AND INFORMATION SCIENCE, UNIVERSITY OF PENNSYLVANIA

STATEMENT OF OMRI BEN-SHAHAR

Mr. Ben-Shahar. Thank you, Chairman Latta. Thank you, Chairman Blackburn, for inviting me, Ranking Members Schakowsky and Doyle and members of the subcommittee, I cherish the opportunity to participate in the conversation. I am a law professor at the University of Chicago and I specialize in consumer law and consumer protection. You will hear today a lot about the dangers of big data enterprise, how websites know our locations, how smart alarms know and predict our vacations, how employers and insurers know our medications, and even Fitbit records our dedication.

We of course all know the data-driven economy delivers enormous convenience and benefits too by offering personalized experience to consumers, but concerns about discrimination, manipulation, data security, and market power and the potential harms they might cause ought to be taken seriously. Still, it is important throughout this inquiry that the basic question, what is the consumer injury, be answered before we begin thinking about what the solution ought to be.

You will probably hear today other speakers call for more transparency on how data is used and secured so as to give consumers more control over their data and allow them to make more informed decisions. Chairman Walden invited such noble proposals of transparency, writing eloquently in an op-ed, quote, it is our job to shine the light on these practices for consumers and ensure transparency in the marketplace so that they can make informed choices.

I would like to spend my remaining 4 minutes or so to try to talk to you out of this transparency instinct. It is not that I don't like transparency or informed decision, it is just that this technique has never worked in any area and it is decisively unlikely to yield any benefit here. I co-authored a book titled "More Than You Wanted To Know" in which I looked at the effect of transparency laws. These are the numerous laws that require companies to give consumers full disclosures to help consumers make informed choices. Mandated disclosure is probably the most common and for sure the least successful regulatory technique in American law. Disclosure requirements, we sometimes call them sunshine laws, have been used for decades as the primary tool for consumer protection to protect borrowers, investors, medical patients, internet users, insurance buyers, home buyers, in every area of the law, and the record confirmed by mountains of empirical evidence is abysmal -- transparency doesn't make a difference.

Transparency requires that companies give consumers disclosures, but consumers are not cooperating. They are not reading or using the disclosures. How could they? The texts are too long and cluttered. Here is a picture of a typical artifact of transparency, Apple's terms and conditions that include their privacy policy, which I printed out and assembled into a 30-feet scroll, 8-point font, mind you, and hung from the top of the atrium at the University of Chicago Law School.

Shoving this monstrosity in front of consumers is that what consumer protection ought to do? If consumers tried to read the disclosures they would of course not understand them and would not be able to put them to profitable use. To use complex information one needs experience and expertise which people simply do not have. Transparency is defeated not because it is a bad idea but because it is so overused.

When you close a mortgage you receive at least 50 different disclosures so that you, quote, know before you owe. When you walk into a clinic or buy a product or enter a website or download an app or eat at a restaurant or check your bank balance you receive disclosures all in the name of transparency. Consumers have long become numb and indifferent.

Any transparency effort in the area of data protection would meet the same consumer apathy. Do you really want to be the authors of an irrelevant policy? Can transparency be done more effectively? If disclosures are defeated by complexity can simplicity save them? Simplification seems like an obvious solution. If disclosures are too long, shorten them; if too technical, use plain language; if poorly presented improve the formatting. Unfortunately, simplification strategies have been tried for as long as disclosures have failed.

In my research I tested whether people who are sharing deeply private information with websites that engage in nasty data practices can be prompted to act more prudently by well-designed privacy warnings. I discovered that no matter how simple, conspicuous, and alarming the warning the consumers receive their behavior is entirely unchanged. Consumers don't pay attention to any of the transparency tools lavished upon them.

To conclude, if members of Congress believe that collection of consumers' data poses risks that require regulatory intervention, I advise that they look for solutions that are outside the popular but unsuccessful repertoire of mandated disclosure and transparency. Thank you.

[The prepared statement of Mr. Ben-Shahar follows:]

**********INSERT 2**********

Mr. Latta. Thank you very much for your testimony this morning.

And, Ms. Klonick, you are recognized for 5 minutes.

STATEMENT OF KATE KLONICK

Ms. Klonick. Thank you. Chairman Blackburn and Latta, Ranking Members Doyle and Schakowsky, and members of the subcommittees thank you for having me here to discuss this important topic.

Every day millions of people around the world post videos, pictures, and text to online speech platforms, but not everything that is posted remains there. Sites like Facebook, Twitter, and YouTube actively curate the content that is posted by their users through a mix of algorithmic and human processes broadly termed content moderation. Until recently, how and why these platforms made these decisions on users' speech was largely opaque.

Over the last 2 years, I have interviewed dozens of former and current executives at these platforms as well as content moderation workers at these companies working abroad in an effort to better understand how and why these platforms regulate content. A summary of that research and my conclusions are the subject of my paper, "The New Governors: the People, Rules, and Processes Governing Online Speech," forthcoming in the Harvard Law Review. My testimony today draws from that expertise and knowledge that I gained in researching and writing that article.

As a threshold matter, when I refer to content moderation I am referring specifically and exclusively to the experience of the user in posting speech to a platform and what happens to that posted content in terms of removal or non-removal. I am not speaking to the algorithm that configures the prioritization, promotion, order, or frequency of how content later appears in users' news feeds or Twitter feeds.

And in that context content moderation happens at many levels. It can happen before content is actually published on the site and when a user uploads a photo a message appears: Upload completed; the video in your post is being processed. We will send you a note when it is ready for review. And the moderation process that happens in this moment between upload and publication largely runs through an algorithm screening that checks for matches in pixel fingerprints between illegal or banned content and the uploaded content. Examples of this include photo DNA for child pornography and content ID for copyrighted information.

Only a very small amount of material is removed through these types of processes and most is published and once published it can be removed in two ways. The first is by platforms proactively using their own moderators, but because of the absolutely enormous amount of posts this is not a feasible method for all but a very select area of moderation such as extremist and terrorist content.

The second way content is removed after publication is also how the vast majority of content is removed, through being flagged as violating community standards by other users on the site. After a piece of content is flagged it will stay up, but a crop screen grab of the content is placed in a database queue where it is eventually reviewed by trained human decision makers. They will look at the offending content and see if it actually violates the terms of service. With that background I would like to use my brief time to clarify four major misconceptions about content moderation. First, that contrary to this hearing's title, the vast majority of content moderation of user content is done by trained human decision makers and who review content only after it has been flagged by other users and not by algorithms or AI or photo recognition.

Second, while users who use sites like Facebook are given a public set of community standards guiding what kinds of content is posted by the site, a separate and much more detailed and much more regularly updated set of internal rules is used by human moderators in making their decisions. These internal rules at these companies are not currently known to the public.

Third, the Facebook and most platforms use one global set of rules with exceptions to comply with the laws of a given jurisdiction to curate content. This means, for example, the definitions of inappropriate sexual activity are the same for users in Canada as they are for users in India as they are for users in France.

Finally, it is critical to note that the ability for these platforms to create this intricate system of governance to regulate content stems from incentives put in place by Communications Decency Act Section 230 which granted platforms immunity from intermediary liability in an effort to encourage sites to remove offensive content while also protecting against collateral censorship of users' speech. In many ways these platforms' self-regulation have very well met the goals of Section 230, but as access to online speech platforms has increasingly become an essential public right new concerns about regulating platforms are being raised. While these and other concerns are undoubtedly present, changes to Section 230 or new regulations that might affect it should be considered with extreme caution and with a full appreciation of the potential damage that could be caused to consumer rights and to free speech. Thank you.

[The prepared statement of Ms. Klonick follows:]

**********INSERT 3**********

Mr. Latta. And again thank you for your testimony. Ms. Moy, you are recognized for 5 minutes.

STATEMENT OF LAURA MOY

Ms. Moy. Thank you. Good morning, Chairman Blackburn and Latta, Ranking Members Doyle and Schakowsky, and distinguished members of the subcommittees.

Consumers are frustrated. Ninety-one percent of adults feel that consumers have lost control of their personal information and nearly 70 percent think the law should do a better job of protecting their information. The law can do better and it should do better. Consumers are in greatest need of greater control when they do not have a choice about whether to share the information in the first place. This is one reason that we have specific privacy laws that protect things like the information students share with educational institutions or the information patients share with doctors. In these contexts and others it is not permissible for companies to simply do what they wish with consumer information as long as they are transparent about it, something we see all too often online; rather, strong privacy protections apply by default. We need similar protection by default in other situations where information sharing is unavoidable as well. For example, when consumer information is shared with a credit agency like Equifax or when consumer information is shared with the provider of an essential communication service like a broadband provider. We may also need protection by default for other types of online actors such as content platforms as they become bigger and more powerful and consumers increasingly find it unavoidable to share their information with those actors as well. This is certainly a conversation worth having.

But whatever specific information sharing problem or problems Congress decides to address it should keep a few things in mind. First, Congress should not eliminate existing protections for consumers' information. This really should go without saying but, unfortunately, in an incredibly unpopular move earlier this year, Congress voted to eliminate strong federal privacy rules that would have applied to broadband access providers.

Similarly, Congress has occasionally considered legislative proposals on data security and breach notification that would eliminate stronger state laws, but consumers want more protection for their information not less. If Congress wishes to improve on the privacy and data security status quo it should start by preserving the protections we already have. And just to touch for a second on net neutrality, the same applies in that context as well. Today's hearing is surfacing some concerns about the power platforms have to editorialize the things internet users read and say, but at the same time the FCC is considering wholesale elimination of rules that prevent broadband providers from doing that. Just imagine how much worse things could get if we start allowing broadband providers to muck with content. Again, consumers in this area need more protection not less.

Second, prospective rulemaking authority is an incredibly important consumer protection tool. After the fact enforcement can be helpful, but an enforcement-only regime does not always create clarity and because it comes only after a problem has occurred it does not necessarily protect consumers from the problem in the first place. Granting rulemaking authority to an expert agency also fosters much needed regulatory flexibility. We do not always know what the next privacy or data security threat will be, but unfortunately we all know that there will be one. An agency with rulemaking authority can respond to shifting threats more quickly than Congress.

Third, consumer protections are only as good as their enforcement so any protections Congress creates on privacy or data security must be accompanied by strong enforcement authority. Right now, the FTC does substantial work on privacy and data security, but with few exceptions it does not have the ability to seek civil penalties for privacy and data security violations. In fact, FTC staff and commissioners have appeared before Congress requesting civil penalty authority to buttress their ability to enforce. Agencies that are tasked with protecting consumers' private information cannot do it without the proper tools. Civil penalty authority is needed.

Fourth, Congress should avoid the temptation to address complex challenges with a one-size-fits-all approach. There are different types of actors on the internet with different roles to play, different relationships with and commitments to consumers, different competition environments, and different abilities to solve problems. If we adopt a uniform regulatory approach to the entire internet we are going to be left with the lowest common denominator, something like transparency with enforcement that just prohibits deceptive practices. That is not good enough. Consumers are asking for more.

I appreciate your commitment to this issue. I thank you and I look forward to your questions.

[The prepared statement of Ms. Moy follows:]

**********INSERT 4**********

Mr. Latta. And again thank you for your testimony this morning.

And Dr. Tucker, you are recognized for 5 minutes.

STATEMENT OF CATHERINE TUCKER

Ms. Tucker. So first of all I would just like to say what a huge honor it is to be invited here today. Thank you very much for the invitation. What I want to do in my 5 minutes is first of all talk about some research I did into an apparent algorithmic bias and then talk about three implications for policy.

Now this particular research topic what we did was we ran a field test on Facebook where we placed an ad which advertised job opportunities in science and technology. And we placed that ad, we also replicated it on Google and Twitter, and we found that the advertising algorithm ended up showing this ad for job opportunities in science to 40 percent more men than women. And on the face of it this seems really quite concerning because obviously this is an area where we would like parity of gender opportunity.

Now I say on the face of it, it sounds concerning, because our research didn't stop there, which is usually how research stops, but instead we actually delved into the reasons why this apparent discrimination had happened. And we ruled out the usual leading explanations which is either that humans are biased, absorb cultural prejudice, or the idea that somehow women have self-inflicted not seeing the ad on themselves by not reacting to it. Instead, if women ever saw the ad they loved it. They clicked on it.

Instead, what actually was going on is all in terms of understanding how the algorithm works, which is that an advertising algorithm basically runs an auction in real time where advertisers bid for eyeballs and there were some advertisers out there that liked to show ads just to women and as a result they pay more to show the ad to women. And because we had set up our ad to be gender-neutral, the algorithm thought it was doing us a favor by trying to minimize our costs and not show our ad to those expensive female eyeballs, but instead prioritize those cheaper male ones.

Now that takes us, you know, to show that actually economic forces actually shape a lot, you know, how we see algorithms work. And I want to just highlight three implications of policy. The first implication is that about algorithmic transparency. Now algorithmic transparency just sounds wonderful, right? Who could ever argue with transparency?

But in this case, let's supposing we could ever decode the pages and pages of algorithms which underlie this ad auction, all we would find is an innocent algorithm trying to save advertisers money. It wouldn't give us really any insight into the potential for bias and I think that is another argument to build on what we have heard earlier, why transparency though just so beautifully sounding is probably not a solution here.

The second thing I want to emphasize is it may be tempting and we sort of, you know, we have heard a little bit of this idea that maybe the problem is not the algorithms, it is the data that feeds them. And I do want to caution the committee surrounding just simply restricting data flows in this economy. I have done some research. I have testified it into the past about the really quite hideous effects that attempts to regulate privacy in online advertising have had on the health and strength of the technology industry in Europe.

We show that they had a 66 percent drop in efficiency after passing regulation and you just have to sort of fast forward 10 years, look at the strength of the American tech industry relative to Europe to see where that has led. I have also done some research in the U.S. We should emphasize that just restricting data in the health arena has actually led to some really quite negative consequences such as hospitals failing to adopt potentially lifesaving neonatal technology saving babies.

Now the last -- so that is why I am worried about restricting data as a solution. The last thing I just want to say is look, in some sense you could write a headline saying MIT professor finds ad algorithm doesn't show job ads, you know, to women, but imagine if I had found that for toothpaste. Would we be that worried? No, we might think, well, maybe men should see toothpaste ads, not that worried about it. So I do want to emphasize again the idea that it really matters, the outcome really matters. Thank you.

[The prepared statement of Ms. Tucker follows:]

**********INSERT 5**********

Mr. Latta. Thank you very much for your testimony. And Dr. Pasquale, you are recognized for 5 minutes.

STATEMENT OF FRANK PASQUALE

Mr. Pasquale. Thank you, Chairman Walden, Blackburn, and Latta -- oh, sorry. Thank you very much, Chairman Walden, Blackburn and Latta and to Ranking Member Schakowsky and Doyle. It is a great honor to be here today.

My testimony is based on my book, "The Black Box Society," in which I distilled about 10 years of research into the role of data and algorithms and argued for the importance of transparency and I am happy to do that today. I want to argue that the use of data and algorithms by large corporations will be at the core of civil rights, consumer protection, and competition policy for the 21st century. And I will go over each of those and then talk about how this committee can play a role in advancing all three of those goals.

First, with respect to civil rights, I was very glad to hear from Congresswoman Clarke about the letter to Facebook with respect to discriminatory ad profiling. That was discovered last year by ProPublica. There were promises it would be addressed. It was not addressed. And I think that shows some of the failures of self-regulation in the area. Also in my testimony I talk about racial disparities with respect to ad delivery and disparities with respect to disability status or a health condition. For example, a credit card company deciding to raise the interest rate on someone once they know that the person went for marriage counseling. I think that is a very troubling sort of thing and we should be able to look into that to get transparency about whether it is happening and to stop it.

Secondly, with respect to consumer protection, Ariel Ezrachi and Maurice Stucke are great antitrust law scholars and they say that given the information, asymmetry between large corporations and consumers, consumers now really exist in a Truman Show. It is like a Truman Show online. They know so much about us, we often know so little about their practices, and they show how consumers can be manipulated by data that they don't know about.

So, you know, we may hear a lot about good personalization online, you see things that you want, et cetera, but there is always a dark side to that. There are things, for example, like vulnerability-based marketing where the marketing could be based on picking out people who are at particularly insecure times in their life or particularly insecure times of day for individuals. And I think this sort of vulnerability-based marketing, predatory loan targeting, all those things are troubling, and not just for traditionally protected groups but also for people, say, in rural areas that might be subject to price discrimination that I discuss in my testimony.

I would also say that with respect to competition, the combination of the power of data in terms of enabling very large digital platforms to decide what consumers see, when they see it, what types of things that they are offered and not offered that

that leads to what I call a self-reinforcing data advantage. What I mean by that is to say that if you are a large platform you tend to have more data. When you have more data you are able to target your things better to consumers. When you are better able to target to consumers more consumers come on board.

It is a virtuous cycle in a way, but on the other hand it does risk getting out of hand and creating the types of asymmetries that are really you can't overcome as a competitor. And we have seen that for example with respect to European action against Google in their antitrust judgment against Google where they talked about Google potentially privileging its own services over rivals in search results in ways that were opaque to consumers.

And I think that we have got to look at those sorts of dynamics and start to address them. It will be hard though. And by the way I would say that one reason maybe why the U.S. tech scene is doing better than the European one, you know, we have to look at these sort of competitive dynamics as well, not just regulation. I would also talk about the black box effect here. I would say that it is very hard for us to know exactly what is going on and we may have only seen the tip of the iceberg here. We may have only scratched the surface.

Now I have painted a very bleak picture and algorithms in this testimony, but there is good news on the horizon. Over the past decade, a number of visionaries have developed a movement for accountability by users of algorithms. It took a combination of computational, legal, and social scientific skills to unearth each of the examples that I have discussed: troubling collection, bad or biased analysis, or discriminatory use of data. And I hope we talk about all three of those things today.

Empiricists may be frustrated by the black box nature of algorithmic decision making, but they can work with legal scholars and activists if we have freedom of information laws and if we enable people to understand better how data is being collected, how it is being used, how it can lead to discrimination. Journalists also have been teaming up with computer programmers and social scientists to expose new privacy violating technologies of data collection analysis and use and they have pushed regulators to crack down on the worst offenders.

I would conclude today by saying that U.S. lawmakers can really help by requiring the openness of algorithms used in many governmental contexts and moving on to empower people to have knowledge of what is going on and how their online lives are being ordered. With that thank you very much.

[The prepared statement of Mr. Pasquale follows:]

**********INSERT 6**********

Mr. Latta. Thank you for your testimony this morning. And Dr. Kearns, you are recognized for 5 minutes.

STATEMENT OF MICHAEL KEARNS

Mr. Kearns. Thank you. Chairman Blackburn and Latta, Ranking Members Doyle and Schakowsky, and other distinguished members of the subcommittees, thank you for the opportunity to testify at this important hearing. My name is Michael Kearns and I am a computer and information science professor at the University of Pennsylvania. I am an active researcher in the field of machine learning and I have consulted extensively on the use of machine learning in the technology and finance industries.

The fields of machine learning and artificial intelligence now play a central role in virtually every sector in which large data sets are present. The number of instances in which the use of machine learning has provided tangible societal benefits, such as in medical diagnosis, is large and growing. Machine learning also increasingly plays a central role in the data collection and use practices of consumer-facing technology companies.

Today I want to discuss data intimacy which is the notion that machine learning enables companies to routinely draw predictions and inferences about users that go far deeper than the apparent face value of the data collected as part of online activities. It is not simply a question of whether consumer-facing tech companies are collecting large volumes of data, such companies are collecting information that provides or allows inferences regarding intimate details about our personal lives.

Search engine queries permit inferences about our physical, financial, and psychological conditions. Social media users routinely reveal intimate opinions, beliefs, or affiliations. For example, a recent study showed that using machine learning, anonymous social relationship data permitted accurate identification of romantic partners for over 55 percent of users. Another study concluded that Facebook's algorithms and models are capable of identifying social relationships of which its users are themselves unaware. And religious and political beliefs can be accurately predicted from apparently unrelated social search and shopping activity.

Consumer-facing tech companies in the United States have amassed an almost unimaginable set of data about consumers which enables machine learning and artificial intelligence to make predictions and inferences about consumer behavior and preferences. These large and diverse data sets are the foundation for effective algorithms and models, and companies compete vigorously to amass or acquire these data sets. For example, search engines provide vast amounts of data about consumers' interests in the manner in which they conduct searches. Similarly, mobile operating system data provides a treasure trove of information regarding virtually everything a consumer does on a mobile device as well as their physical location.

In addition to knowing with whom a consumer affiliates directly, social media platforms are able to accumulate information about who a consumer follows or what he or she likes. However, while the quantity of data is critical to develop accurate algorithms and models, the quality and intimacy of such data is equally or more important in discerning consumer preferences and behaviors. Increasingly, machine learning based algorithms are utilized not only to determine consumer purchasing habits, but also to infer a consumer's emotions, moods, and mental states.

While machine learning is employed most commonly and pervasively to target advertising as we have seen in the media recently, algorithms can also be utilized to generate or incite certain emotional responses. From a privacy perspective, perhaps the most important overarching conclusion is that the intimacy of consumer data cannot be measured by metrics that fail to account for the nature, diversity, and content of the data and, most importantly, its potential uses for modeling and inferences.

It is both common and possible that the highest volume data sources can reveal little about the consumers who generate that traffic, whereas more specialized data can directly and indirectly reveal the most private and personal details about consumers. In fact, the widespread application of machine learning to specialized consumer data sources is deliberately designed to extract personal and actionable insights about both individual users and collective behavior. It would thus be wrong to formulate privacy policy based only on the amount or apparent source of data. One must evaluate the sensitivity of the data as well as anticipate how private or intimate the inferences and predictions that could be made from the data might be. This challenge argues for a privacy framework that comprehensively covers the diverse range of data being used commercially and applies consistent technology-neutral privacy requirements.

Thank you again for the opportunity to testify before you. Machine learning and AI present significant challenges for policymakers because of the rapidly evolving nature of the technology as well as its pervasive use among consumer-facing tech companies in predicting consumer preferences and drawing inferences about their lives. While policymakers should be mindful that machine learning and AI also produce many of the sizeable benefits inherent in consumers' online experiences, such technology enables companies also to both model and shape user behavior. Thank you.

[The prepared statement of Mr. Kearns follows:]

**********INSERT 7**********

Mr. Latta. Thank you very much for your testimony. We really appreciate it. And this ends that portion of our hearing this morning. We will now be going to the questions from the members and I will begin the questioning and recognize myself for 5 minutes. And again I apologize for my 4 weeks of allergies and I hope I get better in the next 4 weeks.

Professor Kearns, if I could start with you. Algorithms are used to produce the results that we see on the internet such as when we do a search or see an advertisement. As policymakers, what are the key benefits and risks for consumers associated with these algorithms that we should be focused on as legislators?

Mr. Kearns. Well, I think the benefits are, you know, pretty obvious to anyone who is a regular user of modern internet technology. The personalization in social media sites, in search engines, and in many other aspects and apps that we use, we all enjoy the benefits of that. I think to me, I think the greatest risks are the kinds of things I talked about which is, you know, there is sort of a distinction about facts about you and things that can be inferred about you from those facts.

And so it is one thing to, for instance, ask about disclosure or discuss what is actually, literally, in the data that is being collected, but that is kind of where the game is being played as far as I am concerned. The use of machine learning allows one to make many inferences that are statistically quite accurate about consumers that aren't written down anywhere in the data about that consumer.

So, you know, to give a personal example, the fact that I am an academic and, you know, use a Mac and drive a Subaru probably lets you guess my political affiliation quite accurately already, and if you knew a bunch of other facts about my online behavior you could probably infer a great deal more. And there are many, many studies these days that sort of establish that fact and this is a valuable thing to technology companies to be able to do that, to do this kind of, I think in one of the other testimonies here, this kind of microsegmentation.

And I think this is the kind of thing that is hard for people to understand and it is even hard for the scientists at these companies to understand the sort of power of this, this sort of predictive power that they have. You know, when these models are built they don't really know a priori and maybe even afterwards exactly what properties of consumers or inferences they are making about them that aren't, you know, they go well beyond the latent data itself.

Mr. Latta. Thank you.

Dr. Tucker, your research shows the tension between how much we say we value privacy and in reality how much data we are willing to share online to connect with friends or get personalized recommendations and coupons. What accounts for that disconnect and how important is the context in what consumers are willing to share online?

Ms. Tucker. Well, I am really thrilled to be able to talk a little bit about this because I didn't get to mention it in my testimony. And this is a so-called privacy paradox that so many people say they care about privacy but then act in ways which doesn't sort of live up to that.

And one thing, we did a little study at MIT where we showed that undergraduates were willing to show really very personal data in exchange for a slice of cheese pizza. And that was even the ones -- and what was slightly disconcerting about it was even the people who said that they really cared about privacy they usually behave in accordance with those norms, but the moment they saw the cheese pizza was the moment they are willing to share the most personal information.

Now I wish I could tell you that I found any group of consumers out there who were not or any group of undergraduates who were not willing to share data for cheese pizza, but I didn't. So as of yet answering your question is hard just because we do see this inconsistency between the way that consumers say they talk about their privacy and actually act out there in the online world.

Mr. Latta. Thank you.

Professor Ben-Shahar, your research indicates that consumers often view privacy policies as confusing and often ignore them, especially from your photograph. At the same time, mandated disclosure has been embraced in many laws and by many regulators. How should we balance the desire for transparency with the results of your research?

Mr. Ben-Shahar. I think we should recognize that our desire for transparency while well-intentioned and makes sense -- very alluring; consistent with all American ideologies; all these transparency laws and mandated disclosure laws pass without opposition in this chambers or in any state chambers; this is the one unifying American law. I think we should also recognize that there is a good reason probably why it is so easy to enact these laws, there is nothing to them.

And therefore I think that it is important to set them, cast them aside and then that would enable us to actually get into the -- I think in my book I give the example of medicine in the 19th century. Almost every disease was addressed by blood-letting. It took the ability or, you know, from the medical profession to recognize that this is, you know, that panaceas don't work. You cannot use that to start figuring out solutions for each individual problem.

And today you are talking, you know, I am invited to talk to you about data policy. I was invited by the FTC and before other agencies to talk about consumer lending, other contexts in which transparency and disclosure is the key regulatory technique and I keep suggesting to them that it is in your area. You have to first ask yourself what the problem is.

I think it is striking to hear what Dr. Tucker and others are finding, that there is -- that statements about the magnitude of the problems are not matched by the behavior and economic reality. Data privacy is a nice kind of buzzword and data security we are really worried about, we can brandish the number of people that were hurt by the different, were implicated by the different breaches that occurred, security breaches.

But what is the evidence about actual consumer harm? Most of the lawsuits that followed, you know, the lawsuits that have followed the Target breach and the Equifax breach were by merchants, credit card companies, banks, they are suffering a lot of the -- there because our laws largely protect consumers from these incidents. So think I do not want to suggest that there is no harm in these areas, but it is critically important to understand its magnitude before we begin to think about solutions.

Mr. Latta. Thank you very much. And since I ran over I will recognize the gentlelady from Illinois, the ranking member of the subcommittee, and also give you a little more time on your questions.

Ms. Schakowsky. Thank you. You know, it is hard to decide who to really focus on because we only have 5 minutes. You know, when it comes to transparency not only don't I take the time to read it, but in order to get to my goal if I don't hit Accept, I Agree, then I can't finish the transaction. So most of the time, for both reasons, I just accept and move on.

So -- but I do want to talk about enforcement and therefore I want to ask Ms. Moy some questions. In Chairman Blackburn's opening statement she talked about shifting privacy from the FCC, the Federal Communications Commission, to the Federal Trade Commission, so I think it is important to understand how the FCC and FTC differ, you alluded to that. But so, Ms. Moy, can you briefly describe the FTC's authority, if any, to issue regulations?

Ms. Moy. The FCC or -- I am sorry, the FTC really doesn't have authority to issue regulations. It can issue rules under -- it can issue Mag-Moss rules, but it is extremely difficult to do that and as a practical matter nearly impossible. It can issue rules under the Children's Online Privacy Protection Act and has done that rather effectively, and the Safeguards Rule under GLBA.

But when it comes to general privacy and data security obligations, the FTC is unable to issue regulations.

Ms. Schakowsky. So the FTC can't use the typical notice and comment rulemaking process to issue regulations about what personal information platforms can collect from users or how those platforms can use that personal information to determine what content it shows to users, correct?

Ms. Moy. That is right.

Ms. Schakowsky. So which means the Commission is limited to bringing enforcement actions after unfair, deceptive practices have been committed and often after consumers have been harmed already, right?

Ms. Moy. Yes.

Ms. Schakowsky. So let's talk about the FTC enforcement tools. In your written testimony you wrote that, quote, the FTC generally can only take enforcement action against entities that use consumer information in ways that violate their own consumer-facing commitments. Can you describe what do you mean exactly by consumer-facing commitments and are you referring to policies like the terms of services and privacy policies?

Ms. Moy. That is right. The bulk of the FTC's privacy and data security authority comes from Section 5 of the Federal Trade Commission Act which authorizes it to prohibit unfair and deceptive trade practices. As a practical matter, the FTC almost never enforces unless it determines that there is deception that has occurred, and it evaluates a possible deception based on something that a company has said perhaps in a privacy policy and then trying to figure out whether or not it has violated that.

Ms. Schakowsky. Even when a platform does violate its own policies the FTC's remedies are limited. As you noted in your written testimony, the FTC cannot impose a fine against that platform. What are the remedies available to the FTC?

Ms. Moy. Exactly. Yes, you know, and as I mention in my comments, I think the authority of an agency is only as good as its enforcement is. And when it comes to the FTC, although it can bring actions for deception when as it relates to privacy and data security, with few exceptions it cannot levy civil penalties against companies that violate privacy and data security commitments. And as a result there is very little in way of teeth when it comes to the FTC's authority.

Ms. Schakowsky. So I know that both Acting Chairman Ohlhausen and Commissioner McSweeny support giving the FTC civil penalties authority and I believe you do too as well; is that right?

Ms. Moy. That is right.

Ms. Schakowsky. And do you think it would be, it would benefit consumers if the FTC had authority then to issue regulations under the normal notice and comment process?

Ms. Moy. I do. I think that the fact that the vast majority of consumers are asking for greater consumer privacy protection and for the law to be stronger in this area suggests that we would benefit greatly from greater authority for the FTC or another agency.

Ms. Schakowsky. Well, so are there other things that Congress can do? I mean you alluded maybe to other agencies to help strengthen the FTC's ability or some other agency to protect consumers.

Ms. Moy. Well, in addition, as of right now the Federal Trade Commission can't actually regulate the actions of common carriers and that is a major problem that particularly with a recent case or a case that is currently pending in the Ninth Circuit it is unclear whether the FTC has any authority at all to enforce the privacy and data security obligations and activities of companies that have any common carrier practice at all. So internet service providers that offer -- whether broadband is classified under Title II or not the FTC may well not be able to.

Ms. Schakowsky. So in the short term what should we be considering?

Ms. Moy. In the short term I think that we do need strong protection, privacy by defaults, ideally, for entities where consumers have no choice but to share information. And I also think that we need to preserve existing protections. We need to preserve existing protections at state law as well as existing protections under regulations like net neutrality.

Ms. Schakowsky. Thank you. I yield back.

Mr. Latta. Thank you. The gentlelady yields back.

The chair now recognizes the chairman of the Communications and Technology Subcommittee for 5 minutes.

Mrs. Blackburn. Thank you, Mr. Chairman, and thank you all for your testimony. It is so enlightening and we appreciate it.

And Dr. Kearns, I am going to come to you first. Thanks for the work you are doing on privacy and around those elements and we have had a lot of focus on privacy here. And earlier this year I had introduced the BROWSER Act and basically it has two guiding principles, things that many of us think are very important. One is that we have to find a better balance on privacy moving toward giving the consumer more information and more control over, as

I term it, their virtual you, their information that is being collected and used and sometimes distributed; and then, secondly, that consumers have the very same privacy expectations across the entire ecosystem. They are not distinguishing between the ISPs and the edge providers, so when we are setting the ground rules on privacy they should reflect that.

So I would like to hear what your thoughts are on those two points. And when we are talking about online privacy do you think that people make that distinction? When we are talking about appropriate balance, where is that appropriate balance within opt-in where the consumer owns that information or either opt-out? So I would love for you to talk about that for a minute.

Mr. Kearns. Yes. These are good questions, hard questions. First of all, to preface I don't have specific policy recommendations on these issues. But as a scientist, when I think about the landscape for consumer privacy the first thing I think about is kind of how actionable the data being collected is and sort of at what level of abstraction it is. And furthermore there is a phrase I like to use which is data triangulation, which refers to the incredible power you can get from having multiple sources of data about the same individual.

So to me, you know, when I think about privacy, the things I worry most about are cases in which there are parties that are collecting sort of very private, intimate data on the one hand and also many different sources of it. So to give an example, you know, by seeing what you buy I can know a lot about you. By seeing, you know, what you search for I can know much more about you. By knowing not only those things but where you are that gives me a great deal of more information. And if you, for instance, let me also maintain your calendar for you then I also know where you will be in the future.

And I think that the, you know, greatest privacy concerns I have are at that level, at the level where people are very directly expressing, you know, things that might be quite private, things that they wouldn't express in public forums, or that they are expressing in a public forum like a social networking service but are completely unaware how strong the correlations are between their own behaviors and their friends' behaviors and their other online behavior. And so I think in terms of helping consumers understand the privacy landscape it is important not to ignore any source of data. I am not claiming that, you know, that ISPs, for instance, aren't also collecting very large amounts of data, but to me, you know, I personally am much more concerned about the data I kind of willingly give away using a search engine, and then also, you know, letting, you know, my operating system track my location online or the presence of beacons in retail stores that kind of correlate my online and my offline behavior.

Mrs. Blackburn. Great.

Ms. Klonick, I want to come to you on economic incentives and the economic incentives that the platforms have to use algorithms to curate selective content. And I think Dr. Kearns used the term microsegmentation as they are looking at that for users, you know, based on this online activity. Would you agree that the platforms are being paid to prioritize certain content over other content? And touch on the free speech implications there.

Ms. Klonick. Yes. Insomuch as advertised content is paid content over their user content, I think that these, you can absolutely prioritize certain types of content. I am not familiar with the algorithmic processes that would prioritize one user's content over the content of another and that they are being paid to do so right now, but the free speech implications of the vast power of these platforms to self-regulate is they are twofold.

One, it has a lot of implications for the user's speech rights in how these private platforms can unilaterally control at what goes up and what stays or goes down on their sites. But also these platforms have free speech rights, arguably, free speech rights, themselves. So their right to create the community at Facebook or at Twitter, for example, is arguably their own First Amendment right.

Mrs. Blackburn. Dr. Tucker, on the economic incentives do you think that some of these platforms should be willing to pay consumers or users more than a free slice of cheese pizza?

Mr. Latta. If you turn your mike on.

Ms. Tucker. Wonderful question. Now this is a very interesting question. So the slice of cheese pizza example was really about the consistency between what people say about their privacy and then how they act.

Now in terms of paying for data there have been many experiments, some of them launched from Cambridge, Massachusetts, where various startups have helped devise, have tried to actually set up markets for data. And the reason that is so attractive is from an economics point of view one way of thinking about privacy is, really, there is a lack of clarity about property rights. So a market for data is an attractive notion.

Now in all of the instances, though I have been really excited at the beginning because of the idea of actually setting up a market for data and paying consumers, all of these platforms have failed for the simple fact that the kind of consumers they attract who want to exchange their data in these markets tend to be, how can I say it, the less commercially exciting consumers. And we have had this problem of actually just setting it up, making these markets work just because we haven't been able to get the right set of consumers.

So I think it is a wonderful idea. I hope one day we will get it to work. We haven't yet.

Mrs. Blackburn. Yield back.

Mr. Latta. Thank you very much. The chair recognizes the gentleman from Pennsylvania, the ranking member on C and T, and

I also yield you the long time too.

Mr. Doyle. Well, Mr. Chairman, this terrible precedent that you have started by allowing everybody to go 2 minutes over, I am going to try to get us back on track and just use my 5 minutes.

You know, when you think about all this technology -- social media, the internet, artificial intelligence -- you know, the most wonderful, horrible invention in the world and as consumers we tend to look at the bright side of all this technology without understanding the dark side. If anybody thinks they have privacy, the only way you have privacy today is, I call it, to go Flintstone, to have the old flip phone, to not be on Facebook or Twitter or any of these social media sites.

But, you know, the reality is for most Americans over 80 percent of the land mass of country, most Americans have only one ISP provider. They don't even have choice when it comes to that. And so they go on their ISP, and it is the only one they have, and they tell you how they are going to use your data and it is about 20 pages long of a bunch of legal jargon that most attorneys probably couldn't understand. And if you don't click I Agree that is it, you don't have access to any of this.

So you don't even need a cheese pizza to get people to give up their information. They want to go online to do whatever it is they want to do online and the only way they can get there, especially if they only have one ISP, is to do that. Now search engines you have some choice and you can read different, you know, policies on search engines of how they use your data and it varies online, whether you are on Google or whether you are on DuckDuckGo or these various sites at least you have some choice. With your ISP most Americans don't have choice. They have one place to go.

And it is kind of ironic that we are here today to discuss concerns about algorithms used by these social media companies to curate content on the internet, but as we speak, over at the FCC the chairman is getting ready to allow broadband providers to block and edit speech on the internet at their discretion relying on public commitment from these providers that they are going to behave.

And given the Ninth Circuit case casting doubt on whether the FTC may even police these broadband companies, it is sort of creating a situation where broadband companies are just free to reign over consumers with impunity and the FTC for all intents and purposes is a toothless tiger. We talk about shifting all this watchdog function over to the FCC --

Ms. Schakowsky. FTC.

Mr. Doyle. -- and they don't really have the ability to do anything on behalf of consumers. Right now, if this law passes on net neutrality next month, basically there is no law of the land, we are just trusting people to behave. They are saying they are going to behave and we are going to take them at their word that they are going to behave.

Professor Moy, I wonder if you can give us some examples of how broadband providers behaved prior to the enactment of strong bright line rules that were put in place by the FCC in 2015?

Ms. Moy. Thank you, Representative. That is a great question. Right, because before we had rules we did see broadband providers, internet service providers, blocking things like Voice over IP, blocking tethering applications, so they could extract more from consumers in monthly fees, blocking peer-to-peer sharing applications. AT&T threatened, I think, to block Face Time unless consumers agreed to pay more for the ability to use that.

So, you know, we certainly have seen examples in the past of ISPs using their power as gatekeepers to prevent consumers from using services that may well want to -- Mr. Doyle. So tell me what recourse would consumers have if the FCC chairman gets his way and removes these protections?

Ms. Moy. It is hard to see how they would have any recourse at all. I mean the FCC plans to rely on the consumer-facing commitments again of ISPs, but it is unclear whether ISPs would actually be required to commit to not prioritizing content, not blocking content. And even if they did make those commitments and then violated them, the FTC, you know, you mentioned the Ninth Circuit case, may not be able to enforce against them. You know, their enforcement authority against ISPs is going to be questionable at best or nonexistent at worse. And even if they could enforce, again they don't have civil penalty authority.

Mr. Doyle. Thank you.

Mr. Chairman, in the spirit of staying within 5 minutes, I have 5 seconds left and I will yield them back to you.

Mr. Latta. Thank you very much. The gentleman yields back. And at this time the chair recognizes the gentleman of the full committee for 5 minutes. I am sorry.

The Chairman. Is that right?

Mr. Latta. The Chairman, the Chairman of the full committee.

The Chairman. Do we have another vote there or what are we on, okay. Thank you. Okay, thank you all, I appreciate it. And thanks for our witnesses. My apologies for having to come and go a bit today, but we do appreciate your written testimony and the answers to our committees' questions.

I guess, Dr. Moy, the question I have because we are concerned about misbehavior by ISPs, I am also concerned about misbehavior by others in the ecosystem of the internet. And it strikes me that on these information platforms we have seen foreign actors try to affect our elections with paid advertisement that is targeted.

We know that there is, in effect, paid prioritization on some of these platforms, right, because you buy advertising, and it strikes me that at least Google, it is an amazing American company, it does incredible work but has about 77 percent market share of search and I have had consumers complain to me about what they believe to be the use of algorithms that have disproportionately affected them.

So what -- and maybe this can go to everybody on the panel, but so if, who governs the edge providers when there are questions about use of private data or -- nothing is private anymore, but your data and how that gets -- and I don't mean this in a negative way, but manipulated use through the algorithms which we are all trying to get a better handle on, so who governs their activities and what enforcement protocols are in place for those?

And I will start with you, Ms. Moy.

Ms. Moy. Great. Thank you so much for the question. So yes, right now those practices are, in theory, governed or regulated by the Federal Trade Commission, enforced by the Federal Trade Commission, again under this idea that they can enforce consumer-facing commitments. But, you know, I think you raise a really good point which is that the growing power of these platforms to editorialize on content is potentially problematic and we should explore possible solutions to that. But in the meantime, the last thing that we should be doing is eliminating protections that consumers have against paid prioritization at the network level where there is very little transparency.

The Chairman. Right. But in terms of other enforcement in the overall ecosystem, if I have a complaint against a search engine or I have a complaint against my social media, I go to the -- my only recourse is the Federal Trade Commission which you have said doesn't have the kind of enforcement authority you would like to see it have, correct?

Ms. Moy. Right, right. Yes, indeed. And, you know, and staff and commissioners --

The Chairman. Do you think there should be greater authority for enforcement over the edge providers or similar to what you would see over the ISPs?

Ms. Moy. I would certainly support adding protections for consumers across the board. I think that there are concerning practices by both types of actors. I would caution this committee against exploring a one-size-fits-all solution to --

The Chairman. Why?

Ms. Moy. Because I think that, you know, again the types of information that various actors have access to is different. The commitments and relationships with consumers that they have is different. For example, consumers are paying dearly for monthly access to the internet with a broadband provider, whereas they often are getting certain other services for free or --

The Chairman. Right. No, it is an exchange of value. Yes.

Ms. Moy. There are certainly differences between different types of actors as well the availability or lack thereof of sharing information with a particular provider or particular type of actor.

The Chairman. So let me ask you a question, because we have also heard before this committee that there is a very high rate of encrypted data that passes through the ISP pipes, if you will allow me to use that term, and that that is encrypted. They don't know what those data are. It is encrypted, it goes through. It is well over 50 percent perhaps so they don't see it, but the other platforms do see the data and can use it and do use it in that exchange as we know. I am not saying these are bad things.

And I think we have heard -- I believe it is Dr. Tucker. I am going to get them to make those nameplates bigger for us old people that have vision issues. But the point is that they can, they see it differently. Can you address that, the differences you have seen in Europe versus here maybe on how our technology has expanded dramatically and innovation here because we haven't cranked down as much, right, on privacy?

Ms. Tucker. Okay. So in the past and this was about 2011 I did research on how some of the early European data privacy regulation really stymied the ability of Europe's ability to create additional ecosystem like we have now. And since then there has actually been follow-up research which has shown that it wasn't just at the beginning but it has kept on going and we have seen an awful lot of lack of entrepreneurship in Europe too.

And so we have seen the failure at the beginning and then the follow-on failure of entrepreneurship, and I think to me that is what has really distinguished what we have seen in the U.S. tech sector.

The Chairman. So we have had, am I accurate to say we have had more of a light touch regulatory approach to the internet up through 2015 from Europe?

Ms. Tucker. I think it is certainly true that we have had a sector-specific touch, right. That we have focused on areas we might care about such as health, private financial data, children, rather than going for a broad brush approach.

The Chairman. All right. I have exceeded my time. Thank you all again for your testimony, it is very helpful in our discussions and I yield back.

Mr. Latta. Thank you very much. The Chairman yields back his time. And at this time the gentlelady from California, Ms. Matsui, is recognized for 5 minutes.

Ms. Matsui. Thank you very much, Mr. Chairman. I want to thank the witnesses for being here with us today.

I have a question, I think, for Ms. Moy right now. In 2015, the Office of Management and Budget issued a memorandum requiring all publicly accessible federal websites to only provide service through an HTTPS connection by the end of 2016, which was last year. HTTPS protocol ensures that a consumer's connection is encrypted from their devices all the way to the federal government's systems. Regular HTTP connections sent in plain text can be intercepted and exploited by anybody or anything between the user and the website including somebody using public WiFi. A study released earlier this month revealed that only around 70 percent of federal websites employed HTTPS protocol.

Ms. Moy, how important are the security standards like HTTPS to protect the confidentiality of internet-delivered data on both federal and commercial websites?

Ms. Moy. HTTPS is very important. HTTPS would encrypt in transit the information that is transmitted via websites. So, for example, if you fill out a web form, for example, perhaps in an application for a service that you might find on a government website and that form contains or asks questions about information that is highly private, such as information about financial status or personally identifying characteristics like Social Security Number, then if the site is not employing HTTPS technology one could mount an attack on the transmission and potentially read the information that was transmitted.

Ms. Matsui. So how would you know whether it employs the HTTPS on the federal website?

Ms. Moy. So this is the type of thing where in a browser bar, you know, you will see up at the top the little, now we have that little icon, the little green lock that indicates trust for HTTPS protocol.

Ms. Matsui. Okay, something what we never look for anyway. Okay, thank you.

I want to talk about embedded networks. Across almost every industry we are seeing a trend towards embedding communications functions into their structures. Applied data science such as a massive internet of medical things, rely on faster, more efficient, and more robust communications with innovative enabling technologies such as blockchain. Blockchain can facilitate the exchange of massive amounts of data, but as a decentralized ledger technology it can make online transactions faster and cheaper while maintaining and protecting data integrity.

Anyone on the panel, how can new digital technologies and applications help consumers improve data security? Anyone want to start on that one?

Ms. Tucker. Well, I have written a little bit on blockchain so I am just so excited that you mentioned it and I am glad that you mentioned it without mentioning bitcoin which is always a distraction.

Ms. Matsui. It is a distraction.

Ms. Tucker. And certainly we have got an initiative at MIT which gives enormous optimism for the kind of process that you are describing where, really, what we call verification costs for making these kind of transactions easier.

Do I have any caveats? My only caveats are that when we have studied it and if we are thinking about blockchain as being a recipe for protecting privacy, that in some sense it can sometimes embolden people to be somewhat more careless about their data surrounding the edge providers who are all who are trying to serve the blockchain. And so, for example, we have seen that the mere mention of blockchain encourages people to share really quite personal information such as telephone numbers and so on without any guarantees of protection.

Ms. Matsui. So they feel like it is much more safe because of the blockchain. They just figure that what they have heard about it that this is a safe way to go?

Ms. Tucker. Yes. That is right. So I sort of have the analogy that it is a bit like once you have your seatbelt on perhaps you drive a bit too fast, that kind of an analogy. And so I think it is definitely a step forward, but we have to realize that of course it is going to interact with other providers and the most will be privacy concerns there.

Ms. Matsui. Thank you.

Did you want to make a comment?

Mr. Pasquale. I would just say very briefly that I testified in September before the Senate Banking Committee and I mentioned in part of my testimony futurist financial technologies such as blockchain. And I think that it is just very important to distinguish between the private permission blockchain and the public permissionless. I have a lot more confidence in the sort of private permission because it involves what I call complementary automation technology complementing individuals rather than replacing them.

So I think that it is, just in terms where I have hope it is more in that latter category of private permission blockchain.

Ms. Matsui. Okay, thank you. And I see my time is expired.

I yield back.

Mrs. Blackburn. [Presiding.] The gentlelady yields back. Ms. Matsui, I just mentioned to counsel that we may want to secure his Senate testimony and submit that into the record in coordination with your question.

Ms. Matsui. Thank you very much.

Mrs. Blackburn. Agreement? So ordered.

Mr. Shimkus, 5 minutes.

Mr. Shimkus. Thank you, Madam Chairman. It is great to be here. I got to listen to your opening statements. I found them all very interesting. And then I had to run upstairs to do energy markets and interconnectivity and then I came back down here, so I may have missed a few issues.

I just want to put on the record on this whole net neutrality debate it is just, for a lot of us it is what is the enshrined law by the legislative process versus what a regulator decides what to do. And what we are seeing now with the passing of the Obama administration, and the Trump administration, is I kind of explain to my constituents it is a pendulum. We are going to do it this way, now we are going to do it this way, now we are going to do it this way, and to stop the pendulum you have to pass a law. You have to enshrine that into a statute and I would encourage my colleagues to come together to do that.

I also want to incentivize build-out. I like more pipes versus less pipes and I don't want the government deciding how one pipe should be structured. I would rather have so many pipes that everybody gets what they want when they want it at the speed that want it and if you are a market-based conservative you have got to send a price signal.

And then the other issue on that is this whole, part of this was kind of paid prioritization or we are talking about so small of lag of time that I can't even use the proper terminology. But would I rather have lifesaving telemedicine go fast versus a Three Stooges video? The answer is yes, I would. So I just want to put that in the guise of some of the debates based upon what the FCC is considering. And then I want to segue real quick to this whole -- this is a fascinating panel because you all have done, brought pretty much a different focus and sometimes there is similarities on privacy, on algorithms, on data.

So I want to use this example. Over the Thanksgiving break I visited Washington University, a major medical facility in St. Louis, and so I briefly drew my little DNA strand, right, here. And so the question with data is in the healthcare arena we want to go to drive to personalized data, I mean personalized medicine, and personalized medicine means we understand the DNA sequence and we can pull that out. So then a cancer patient, we don't have to try 15 different types of cures, we can direct it.

Now that creates a lot of issues public policy-wise. One issue is the data collection. The other one is data sharing. The other issue is privacy. And when you are doing medical research, I mean you are really trying to share that data, that DNA sequence of this one case across different major schools of medicine across the country and probably across the globe.

So that goes to a lot of our individual comments I kind of want this to happen. I really believe in personalized medicine. I think it is going to be a huge savings and I think it helps treat the patient quicker and return them to a very, you know, return life. And we have these hurdles that we are all discussing here.

Anyone want to weigh in on -- there is, let me -- Mr. Pasquale, and then I will go to Dr. Tucker. I got about a minute, 2 minutes left.

Mr. Pasquale. I will be very quick to say that I completely agree with you and I think that, you know, we have talked to -- I run a health law podcast with Nick Terry called "The Week in Health Law" and we talked to several people who are law and policy experts in this type of area, sensitive health data, and we get a lot of good advice on, you know, how can we develop best practices in order to enable data liquidity, data flow between institutions.

But I would also say, you know, based on some of the great work done by Sharona Hoffman in her article "Big Bad Data" that sometimes if we don't have good data practices so we know where data comes from and where it is going to that may impede the scientific validity of some of the findings. So I think we have heard a lot about privacy impeding innovation, but there are ways in which good data practices, good record keeping can actually help promote innovation as well and promote scientific validity.

Mr. Shimkus. Thank you.

Dr. Tucker?

Ms. Tucker. So I have a study coming out, it is forthcoming at Management and Science where we actually look at different types of regulation and how they promote or don't promote the kind of personalized medicine you are talking about. And what we found there was that basically just focusing on consent was really quite harmful to patients being willing to adopt this kind of or sort of give this kind of unique data in a cancer treatment setting.

What did seem to work though was actually giving control to patients and there were some states that actually experimented with creating ownership or property rights over genetic data and we have actually seen quite a bit of efficacy in terms of promoting personalized cancer treatments in those states.

Mr. Shimkus. Anyone else want to weigh in? I really enjoyed -- again I am having a hard time too with Mr. Ben-Shahar on the statements of, I mean how many of us get financial booklets after the fiscal year and how many people throw it away, I bet you 99.99 percent of all people who get those booklets on what you should know. And I think it is a protection. It is really a protection for those people who are controlling our data. Okay, we have done it. We have given you the information, now it is your fault if you don't follow it.

So it is a great hearing. I appreciate everybody being involved. And I yield back my time.

Mrs. Blackburn. The gentleman yields back and, Mr. Green, 5 minutes.

Mr. Green. Thank you, Madam Chairman. And I want to thank our two chairs and two ranking members for the hearing today and as well as our witnesses.

It is pointed out that personalized content that we all see on various online platforms is curated by both humans and algorithmic technology. However, the potential for harm from algorithms can be particularly difficult for Congress to address and thus we should be focusing on it.

Professor Kearns, in your testimony you point out that machine learning-based algorithms can be used to determine a consumer's emotions at any given point in time. How do you monetize that?

Mr. Kearns. Well, the short answer is I don't know. But certainly if I can shape people's moods and it seems plausible people might be more willing to shop if they are in a good mood rather than a bad mood that might be one way that I could monetize it. I think more generally though, you know, knowing detailed, fine-grained information about people's mental and emotional states, you know, in addition to, for instance, knowing about medical facts about them and their fitness level and their financial health, et cetera, I mean it has, you know, clear sources of monetization.

And some of my colleagues on the panel have mentioned some of the negative ones already such as targeting groups that are particularly vulnerable at a particular time. There is a great deal of documentation, for instance, on, you know, kind of predatory loan practices online, you know, in the arena of for-profit education, for example.

Mr. Green. Okay, thank you.

Professor Pasquale, if a person often does online searches for phrases that might signify challenging financial circumstances such as financial counseling, how might that change the ads and the search results that they see online?

Mr. Pasquale. Oh that is a terrific question. And one of the big worries that a lot of advocates have is that we can route people into different opportunities. So, for example, if you have exactly the type of searches that you are mentioning someone might be routed towards payday loans, others might be routed away from them. Now to Google's great credit, I think, 1 or 2 years ago, working actually with Georgetown, they did invoke, involve -- they started some self-regulation where they said we are not going to have certain ads on that are over 36 percent APR. And I think that is very important, but I also worry that, you know, kind of competition concerns might arise if, for example, Google owned its own finance company that had a business model that would be advantaged by that particular rule.

So I think we have to balance, you know, we have to both encourage tech giants to try to self-regulate to avoid the type of tracking that you are invoking, but we also have to have outside authorities to be able to watch that self-regulation as well.

Mr. Green. Or just so the consumer knows that, you know, that is being done and you might not be getting some other offers, that somebody else is making that decision on what they are presenting to you.

Another question I have, you mentioned in your testimony that in 2016 after Facebook was found to enabling discriminatory housing ads it promised to change the system to address that issue but has not done so. Could you talk about efforts that Facebook and who might require Facebook to fix this problem and why they may not be successful?

Mr. Pasquale. Yes. I think that the issues here are it is a complex ad ecosystem and so there is lots of different moving parts in the ads, but I think that when we -- what is disappointing is that there was this expose in ProPublica, there was a lot of attention to it. There were pledges to do better, but we just saw in the past week or so that the same people that exposed the original problem that they are saying it hasn't been solved.

So I think that is again another example where we have to empower either state or federal regulators to actually have some teeth and to impose some of the penalties that would actually lead to a positive response.

Mr. Green. As I found out in this job, everybody needs the boss and has to answer to someone. So we don't have an agency that can do that right now with Facebook if they agree to do something and does not do it?

Mr. Pasquale. I think that there are, there is possibilities with respect to say the deceptiveness or unfairness authority at FTC. I would also have to research with respect to the Department of Housing and Urban Development and its own enforcement practices, but that is not something that I have personally looked into so I would have to look into that. Yes. And I could send that later on to the committee, yes.

Mr. Green. Professor Kearns, you advocate for a policy approach to the extraction of consumer data that is technologically neutral and accounts for the sensitivity of the data collected. My question, can you elaborate on what you think that policy might look like?

Mr. Kearns. Yes. I mean, first of all, maybe let me take the opportunity to say one thing that I think has been running through my head but I haven't been able to get out yet, which is especially on issues of discriminatory behavior by algorithms I do think that there are scientific things that can be done to address this and there is a, you know, not small and growing community of AI and machine learning researchers who are trying to design algorithms explicitly that meet the various fairness promises and guarantees.

And it is still very early days, but this sort of idea of endogenizing some kind of social norm like fairness or privacy inside of an algorithm I think is extremely important, because while regulatory and watchdog agencies will always be very important, you know, the way a computer scientist would put it is they don't scale, right. So if instances of malfeasance or privacy or fairness violations have to be caught by human organizations looking at, you know, specific instances or behaviors they just won't keep up, right, because the tech companies are doing this at massive scale in an automated way.

In terms of what can be done, you know, I think it is possible to audit algorithms for various kinds of behaviors without compromising the proprietary nature of the models or algorithms used. And a rough analogy I would offer are kind of the stress tests that banks have been subjected to on Wall Street where, you know, you have to demonstrate certain properties of behavior of your algorithm but you are not, you know, releasing the source code for it.

And I, you know, without having super-specific suggestions in that regard, I think that that is a promising general direction for policy and one that can balance between, you know, a company's legitimate right to preserve their intellectual property and consumer and societal concerns about the behavior of those algorithms.

Mr. Green. Thank you.

Mr. Chairman, I know I am over time. I appreciate your courtesies.

Mr. Lance. [Presiding.] Thank you very much, Mr. Green, and I recognize myself.

Ms. Klonick, in your testimony you mentioned choice as a key part of regulators' decisions not to pursue Title II-like regulations for online platforms. Title II-style regulations may be inappropriate for edge providers or for others in the internet ecosystem as well. However, some have argued there are fewer choices among online platforms because each website or application serves a specific audience with a specific service. Would you please comment on that? Thank you.

Ms. Klonick. Yes. I agree with that statement generally that specific platforms speak to a specific audience. But there is an enormous and incredibly important distinction to be made here and that is that there is a huge difference between companies that have kind of natural monopolies like ISPs and then content platforms like Facebook and Twitter.

And the former kind of a piece of the pipe, or to put it in terms of speech, they are kind of the printing press and you don't want the printing press rearranging letters or blocking out sentences. You want it to be content-neutral to a certain extent and but you do want the paper or the writers or the editors who use that printing press to be able to make decisions based on the content and that is something why what we are talking about today is so important.

Mr. Lance. Thank you. If there are fewer choices among these platforms how does that change the evaluation of the platform's ability to moderate content? Does it make it more or less troublesome in your judgment?

Ms. Klonick. Yes. I think that as Representative Doyle said earlier that one of the issues here is that there is a lack of choice between certain types of providers, but on these platforms right now there is just a plethora of choice. I mean Twitter might have a monopoly over 280 characters of text and Facebook might have a monopoly over a kind of like a relatively safe, family-safe community, but there are plenty of other presences that are currently online. Of course if that changes in the future and the taxonomy of what these different platforms are able to provide and what users use them for and how they end up having a monopolization or not over broader areas, then I think that that is something that can be revisited.

Mr. Lance. Thank you very much.

Professor Ben-Shahar, as many of the online platforms we are discussing today offer their services free of charge as consumers, how do we as lawmakers evaluate the appropriate balance between personal privacy against convenience?

Mr. Ben-Shahar. Thank you very much for the question. I was hoping to be able to say a few words about that. I think we should be very careful not to change this grand bargain, people paying for excellent services that they like very much not with money but with their data. And it would be a, I think, disaster of consumer protection if we changed that, if people -- if you ask consumers in the aftermath of some reform that removed that bargain and made them pay for things like Google, Facebook, and other things with money, if they feel that they were helped I think they would say in unison, no, don't do this.

In that sense I think the bargain and the underlying bargain is an excellent bargain. Now there are worries that of course arise and I think this is the ultimate, the foundational problem of data policy. It is not privacy or security, it is competition. It is the fact that there are very few companies that dominate the central forum in which these exchanges occur -- Google, Amazon, Facebook, and maybe a few more small players.

I am not so worried about the ISPs. They, notwithstanding the fact that on broadband there is some local monopolies, there is great competition from mobile, but these big three, or big four if you throw in Apple, big five if you throw in Microsoft, have a lot of power and the FTC has failed, for example, last year, to intervene in something that the Europeans thought, I think rightly, as raising antitrust concerns.

So to conclude, I think that the concern for consumers is, will arise from lack of competition and concentration not from privacy and security.

Mr. Lance. Thank you very much and I yield back 42 seconds and I recognize Mr. McNerney of California.

Mr. McNerney. Well, I thank the chairman and I thank the witnesses. Sorry, I missed some of your testimony a little earlier. Professor Moy, what do you think the benefits of the current FCC rules for consumers and small businesses are regarding net neutrality?

Ms. Moy. Great, yes. So I mean that is a great question. I appreciate that question. The current rules enable small businesses to reach consumers. That is the short answer to the question. You know, if we didn't have rules that prevented ISPs from paid prioritization and blocking, then it would be much more difficult, potentially, for small businesses to reach consumers.

Mr. McNerney. So you would agree -- or I don't want to put an answer in your mouth -- would you agree that that would be harder for small businesses to innovate if the FCC chairman's proposal is adopted?

Ms. Moy. Yes. You know, and it might even be very difficult for a business to know whether or not it is being throttled if it is being throttled. The draft order has transparency provisions in it, but it is unclear whether the transparency provisions would be consumer-facing or in fact if some companies could fulfill those by just turning over information about their practices directly to the FCC.

Mr. McNerney. Well, that sort of leads, already answered my next question. But the new rules or the new regime would require or ask businesses if they feel like they have been subject to anti-competitive practice to go to the FCC to resolve their problems. How quickly do you think the FCC could response to those sorts of requests?

Ms. Moy. I mean if it could respond at all, I mean, well, I think the question is whether it could respond at all, right. So there are many practices that might seem anti-competitive but not raise to the level of an antitrust violation. So, for example, if an ISP were throttling a service that an innovator is introducing into the market but that doesn't compete directly with the ISP service of a phone or internet provision, then that practice might look anti-competitive but might not be considered an antitrust violation.

Also if, you know, if a company were to try to bring an action in court, you know, I think there is this idea that companies might be able to bring antitrust actions in court, but antitrust actions in court take many years and may cost potentially millions of dollars to mount against a major incumbent. And that can be, you know, that is a barrier that really creates impossibility for a small business or --

Mr. McNerney. Sure. And what sort of penalties could the FTC impose and would they be effective?

Ms. Moy. Right. I mean so again the FTC's primary authority when it comes to enforcing something like net neutrality, if it could enforce net neutrality again, you know, and I think for all of the reasons that we have discussed repeatedly, including the FTC's lack of authority over common carriers, it is questionable whether they have the authority at all, but most of their authority would come from the ability to prohibit unfair and deceptive trade practices and there is no civil penalty authority in that area.

Mr. McNerney. So under Chairman Pai's plan, broadband providers are not required to disclose the practices at the point of sale or on their website but they can give those practices to the FTC and the FCC and they would in turn put them on their website. Is that sort of disclosure viable?

Ms. Moy. So, you know, I mean I think I would say again, you know, I think as an initial matter it is worth remembering that the disclosures alone are not necessarily, are not going to be sufficient particularly when it comes to when you are in a situation where a consumer only has access to one broadband provider.

But when there is a choice that is available to the consumer and they might rely on disclosures to make a choice between two different providers or between multiple providers that information really does need to be consumer-facing. I was, in fact, on the task force at the Consumer Advisory Committee, the FCC's Consumer Advisory Committee that designed the so-called broadband nutrition label that Chairman Pai is planning to do away with, you know, and we did think that in a situation where a consumer might be considering adopting one of two different services or one of two different service plans it would be extremely important for them to have easy-to-read information about the actual performance of that service package.

Mr. McNerney. I had a couple of questions for Professor Kearns. With regard to machine learning there is going to be benefits in all sorts of areas, but are there areas where machine learning techniques should not be used?

Mr. Kearns. Well, yes, I think so. And there is, you know, a large and growing community of AI and machine learning researchers who are trying to debate those sorts of issues. You know, one logical extreme, there is the notion that any decision that really, you know, should lie with a human just because of moral agency shouldn't be made by an algorithm.

So one example that is commonly offered is in automated warfare that even if we could design algorithms or learn models that, you know, made more accurate decisions about whether to fire on an enemy that perhaps we shouldn't do that because the decision to do that should always lie with a human who has the moral responsibility for that decision.

So I think, you know, that is an extreme that I think I would agree with. The harder cases I think are cases in which, you know, machine learning is demonstrably effective yet making difficult moral decisions like in criminal sentencing and to, you know, one could arguably ask about things like, you know, college admissions or loan decisions and the like.

And so, you know, my view right now is that we are at the very beginning of a very difficult debate about the extent to which decisions that have been made historically by humans and by the way, you know, historically also exhibited biased privacy decisions, et cetera, when they were being made by humans and turning over them to machines where the tradeoffs are going to be different but there will be tradeoffs, right.

And there is always this tension in machine learning between accuracy which is, you know, right now essentially what is almost always optimized for and other things like privacy and accuracy like -- I mean privacy or fairness, right.

Mr. McNerney. Well, I have really gone over my time.

Mr. Kearns. Okay, yes.

Mr. McNerney. So I am going to have to interrupt you and yield back. Thank you.

Mr. Lance. Thank you very much. The chair recognizes Mr. Johnson.

Mr. Johnson. Thank you, Mr. Chairman.

Mr. Pasquale, when we talk about how companies interact with consumers and handle consumer data we often talk about transparency, that is, being transparent with business practices. In some industries there are actually transparency rules that require companies to disclose certain information. For example, ISPs have to disclose a slew of information about their business and network practices. Are there any rules that require companies that use algorithms to be transparent about how they work?

Mr. Pasquale. So it is a very narrow range of requirements. So, for example, if you look at the online lending space there has been some caution about certain forms of automated underwriting using what is called fringe or alternative data, data beyond, you know, what is usually used by FICO or other entities like that because under FCRA it can be a requirement of explanation under the Fair Credit Reporting Act with respect to some of these, like giving the reason codes for why an automated decision was made.

But in general it is a zone of great opacity. We just don't know. That is why I titled my book "The Black Box Society" because there are so many rules there, so little sense of what is going on there. Yes.

Mr. Johnson. Okay, all right.

Mr. Kearns, Professor Swire from Georgia Tech, my alma mater by the way, it is where I learned about networking, concluded that applications such as search engines and social networking services collect data providing greater consumer insight than ISPs. Do you agree with that conclusion?

Mr. Kearns. Yes, I do.

Mr. Johnson. Okay, care to expand?

Mr. Kearns. Well, in addition to the aforementioned encryption that, you know, occurs with the vast majority of data that ISPs carry, you know, there is the additional fact that I don't think it has been mentioned yet that it is at the packet level. So, you know, and the way internet routing, packet routing works is that longer messages, whether they are actual text messages or they are a web search or they are an audio call, are divided into these tiny little fixed-size packets which then travel possibly different paths through the network.

So, you know, just going back to a comment I made earlier, this sort of actionability of data at that level, if, you know, if half or more of it is encrypted and it is also traveling in these little bite-sized pieces and you are carrying a phenomenal amount of that data over your network, if you ask me whether if I am trying to figure out who somebody is and what to sell them and what their mental and psychological condition is, I would much rather have search engine data or Facebook data than packets at the network level.

So this is basically what I mean by, I think, you know, it is, from a privacy perspective it is less concerning to me that the data that is being collected by the edge services.

Mr. Johnson. Okay, all right. Continuing with you, Mr. Kearns, then, my understanding is that approximately 80 percent of internet traffic is encrypted. You just talked about encryption a little bit. That limits what ISPs see regarding consumers' online activities. In contrast, by their very nature, don't edge providers largely have to interact with consumers' unencrypted data?

Mr. Kearns. By definition, yes.

Mr. Johnson. Yes. Well, doesn't that give edge providers much greater insight into consumers' preferences, habits, choices, beliefs, that kind of stuff?

Mr. Kearns. Yes, it does. I mean I think the right way to think about it, let's say, back in the old days of telephony is, you know, would you rather see, you know, would you rather see the raw analog signal and try to figure out what the conversation is from that or would you rather have that analog signal rendered through a speaker so that you could actually listen to the conversation, right? And this is an imperfect metaphor, but I think it is a good one.

You know, another thing I might offer is if I am just trying to describe an image to you would you rather I go pixel by pixel through the image and tell you the color value of it, or would you rather me describe it to you and say, well, it is an outdoor image? There is trees. There is a lake. There is a family picnicking. And so, you know, by definition, what the end services are getting and what users want to give to those end users are these, this much higher level data that is easy for humans to understand and model.

Mr. Johnson. They want to see it all put back together again.

Mr. Kearns. Yes, exactly. And you are just kind of not easily getting that at the network level because of the encryption and because of the fragmentary nature of packet routing.

Mr. Johnson. Right, right. Okay.

Well, Mr. Chairman, I yield back a full 10 seconds.

Mr. Lance. Thank you, Mr. Johnson. The chair recognizes Ms. Eshoo.

Ms. Eshoo. Thank you, Mr. Chairman, and thank you to the witnesses. I read all your testimony last night, listened to all of you today and I want to make some comments about this hearing. The title of it is very interesting and it is an area that needs to be examined.

The word privacy has come up many times, certainly net neutrality and references to it have come up. Strong enforcement has come up. But when you look at the backdrop and the broader stage on which this hearing sits, look what is happening in our country. In a flash, like lightning, privacy was ripped away, the privacy protections were ripped away from the internet.

So all of the happy talk of some of my colleagues on this committee about privacy and the sanctity of it that was forgotten when that vote was taken and the American consumer, I think, has really been hammered as a result of it. I think that, Professor Moy, you made a very important point when you said that the last thing we should do is to repeal, and that has happened.

It was very interesting to hear the description of what has taken place in Europe with what they have done with the internet and what we have done and how the internet has flourished in our country just on the eve of the chairman of the Federal Communications Commission getting ready to rip away the protections that are there that have made it open, free, accessible. So I think there is some political cross-dressing here today, with all due respect, not by the panelists, but I think by some of the members.

And the term a strong enforcement has been referred to, but I don't think strong enforcement is something that you pick and choose, because we are lawmakers and unless there is enforcement then the law is not worth the paper that it is written on.

I take heart from what Professor Kearns spoke of because in this whole issue of algorithms -- and let's keep in mind these social platforms are free. They are free. They are not like the ISPs. In the ISPs there must be, I think, only three happy outfits in the entire nation on the eve of what Chairman Pai is doing and that is relative to net neutrality and that is Comcast, AT&T, and Verizon. They are the happiest. I don't know anyone else that is for what he is planning to do to the internet. But I do think that the -- it is very interesting to me that you have raised the issue of auditing algorithms.

Now I think that truth has always required transparency. We don't, I don't think, as a committee, really know how to get socks on the octopus, so to speak, here because it is complicated. Free speech is central to us, but we also know that there are bad actors that have used the best of what we have invented to divide us and something needs to be done about that. There is no question in my mind, and the chairman of the full committee raised that as well.

So how close, Professor Kearns, do you think we are to this what you raised, the auditing of algorithms?

Mr. Kearns. So I think we are close. So in particular, you know, many of the instances of discrimination, for instance, in algorithmic behavior were actually discovered by groups of researchers who are effectively doing their own auditing, you know, doing kind of field experiments using services that have algorithms underlying them, testing their behavior and demonstrating, for instance, they have some particular type of bias.

There is good research being done on again internalizing notions of fairness inside of algorithms. And just to be clear here, I think most instances of discrimination in algorithmic behavior are not the result of any evil by the researchers and scientists at these companies. It is just that when you optimize your model for predictive accuracy you shouldn't expect it to have any other nice properties either, so you need to, you know, you need to actually specifically put those properties in your code if you want them to have it.

You know, in the privacy arena there is a very strong notion of, you know, kind of internal privacy of an algorithm known as differential privacy that is kind of starting to finally get out of the lab and be used, for instance, in the latest version of Apple's iOS. So this stuff is happening and the tech companies are participating in, you know, the dialogue and in developing some of the science. It just needs to be kind of taken seriously at scale by those companies.

Ms. Eshoo. Well, I am encouraged by what you have just described and I want to pursue it as well. If there is more information that you can get to us on it, I certainly would welcome it. And with that Mr. Chairman, I yield back.

Mr. Lance. Thank you very much. The chair recognizes Dr. Bucshon.

Mr. Bucshon. Thank you, Mr. Chairman.

Professor Kearns, this is a little bit different line of questioning but important. Is it feasible for your cell phone or an app on your cell phone to listen in on your conversation and collect data?

Mr. Kearns. Yes.

Mr. Bucshon. And are you aware that that is happening in our country, in everywhere? I will give you an example of why I think that this is happening and it is an issue that we really haven't touched on today as part of data collection.

Mr. Kearns. My default assumption is that unless I have taken explicit pains to arrange otherwise that when I use an app on my mobile phone it is recording at least the data of my interaction with that app and possibly many other aspects of my usage of the phone as well.

Mr. Bucshon. How about when you are talking? Like right now my phone is sitting here and there is a speaker and I am talking and is that data, is what I am saying potentially being collected?

Mr. Kearns. With or without the microphone on.

Mr. Bucshon. Correct, with or without. Well, the question is the definition of on, right, because that is being made by the company that makes the phone. I mean it has been shown recently and it has been on, I think, Wall Street or somebody reported that you can turn off essentially everything on your phone and you are still being tracked. So the speaker is important.

Let me just say this, and this is the reason this came to me is because my son who is 24, he lives in Chicago, he was standing around with some, a couple, with a friend at work, a person at work. Nobody was on the internet. He was talking about, and I can't remember specifically what it was but it was about shoes or something and the next day he had ads for that exact thing on his feed. He didn't do a Google, he didn't do any search. I don't want to single out a company, but he didn't do any search at all. All he did was talk in the presence of his microphone on his phone. Do we know if that is happening?

Mr. Kearns. I am not a security expert, but I do know that there are more instances these days of situations in which, you know, the operating system on your mobile phone communicates with beacons in retail stores and this is how one often experiences, you know, why even though I didn't do a search on some product at all but I happened to be in the store yesterday, the physical retail store --

Mr. Bucshon. Yes, they can do that.

Mr. Kearns. -- am I not, you know, and this is because they are now starting to install so-called beacons in these stores that interact with the operating system on your phone and so then the retailer knows that you were there.

Mr. Bucshon. If you were in a shoe store they know you were in a shoe store.

Mr. Kearns. So, you know, my feeling about these things is that the way technology is, is anything is possible, right. And then the question is, is it widespread and who is doing it and it is kind of for deliberately nefarious purposes or is it, you know, just advertising, quote unquote?

Mr. Bucshon. I mean it is important because I am a member of Congress and I have confidential conversations all the time with my phone and I am not on the internet. And so that is a question. I had mentioned this to my staff by the way when I went back to the office and they go, oh yeah, that has happened to me. I mean all the young people are like, oh yeah, that happened to me before.

So I just thought that was something that we need to, really, also as far as collecting data and then analyzing like you have described, I mean I think what we really need to think about, not only when you are actively on your phone but whether or not through your -- and I am not a conspiracy theorist or anything, right -- through your actual speaker that you can be monitored.

Mr. Kearns. Yes. I mean and I think we are also voluntarily heading this direction in the form of home devices like, you know, Echos and, you know --

Mr. Bucshon. Yes, right. That is obvious, right.

Mr. Kearns. -- in which, you know, are kind of sitting there all the time recording.

Mr. Bucshon. Right.

Professor Ben-Shahar, you stated that consumers ignore privacy disclosures. How would you suggest we inform consumers that they have given consent to their data being collected? How can we do that?

Mr. Ben-Shahar. I think consumers understand in general what is going on and indeed a lot of the surveys suggest that they know that a lot of their information is being collected. They are not surprised when they find out that yet another practice is prevalent, for example, that now these home butlers, the Google Home or Alexa is listening to everything that is going on. I think that consumers by now have figured out that this is going on and so there is not much that we can tell them that they don't know.

Now there are specific things that are going on that defy consumers' expectation. And if the expectation is created in an affirmative way by your smart phone or by Google or by other service, for example, they give the consumer the impression that they can turn on or turn off some kinds of surveillance or some kinds of data collection and it turns out that they can't, that even if they did what they were supposed to do and had the reasonable understanding that they are not going to tracked in a particular way, they still are, that is an FTC issue. That is an issue of --

Mr. Bucshon. Well, that has happened. It has just been written in the papers recently that it has happened.

Mr. Ben-Shahar. To the extent that that is happening that should be, I think that there are tools in our law both in contract law and in consumer protection statutory law to take care of these kind of things. I don't know, you know, maybe other panelists know better. I don't think these things happen too much for the simple reason that it all costs nothing for the services to let consumers know what is going on. Consumers don't care. They are not going to bother, change the settings or re-change the settings every time there is a new version of the software.

Mr. Bucshon. Thank you. I am out of time. I yield back.

Mr. Lance. Thank you very much.

The chair recognizes Congressman Flores.

Mr. Flores. Thank you, Mr. Chairman. I appreciate all the panelists for joining us for this important hearing today.

The first question I ask, I mean one of the things that is obvious is that data is pulled from everywhere whether it is data services, your mobile phone, your Alexa, whatever, operating systems, and social media platforms. So my question is this for all of the panel. I am going to start with Professor Kearns and then I am going to ask a couple of other questions and we will come back to the panel if we have time about this issue.

So the question is simply this. What are your thoughts as to whether or not Congress or policymakers need to establish a consistent legal and regulatory framework for how this data is obtained and used?

Mr. Kearns. Well, I will be brief so other people can talk too. But I mean as per my earliest remarks as a scientist, so I am not a policymaker, I am not a lawyer --

Mr. Flores. Right.

Mr. Kearns. -- but from a scientific perspective, to me the most important thing is not sort of, you know, how much data you have measured in petabytes. It is not kind of whether the data came from this service or that service or this app or that ISP. It is what are the actionable insights about consumers and what are the facts about their lives that you can infer from that data.

And as a scientist I don't see an easy way to carve that up into little subdomains and say like, oh well, you know, because we just, the truth is we don't know, right. These companies themselves are figuring out just now how powerful AI and machine learning techniques applied to all kinds of data are.

Mr. Flores. Right. Well, the challenge is, is that policymakers and regulators typically move way behind the speed of technological change. And so what I am trying to figure out is how do we get in front of this or do we need to even worry about it? And I will come back to the rest of the panel on this question in just a minute, but I do have two other questions for Professor Pasquale first.

In your testimony you noted that bottlenecks can threaten competition at any layer of the network not just the physical layer provided by the ISPs. And so the question is this. Can you elaborate on the potential bottlenecks other than the ISPs, beyond the ISPs?

Mr. Pasquale. Sure. So I did a 2008 article called "Internet Nondiscrimination Principles" and what I tried to do is to say that the same type of concerns that are motivating people to advocate for net neutrality should also be looked at, at the social layer, at the search engine, at the app store level. And particular examples, there are two examples related to China that I think are really interesting and I discuss in my book. One is that someone developed an app called "In a Permanent Save State" and it was a game that was also a critique of Apple and its use of certain Chinese factories and labor. And the Apple app store rejected it over and over again and they couldn't really understand why that was happening.

Similarly, there is a case called Langdon v. Google where someone wanted to buy an ad titled "China is Evil," and there was, I thought, a relatively arbitrary decision by Google to say no, we are not going to sell you that ad. And so I think those are very concrete examples of a much larger problem where I think that we have to be much more imaginative as academics and as policymakers in seeing the connections rather than seeing the separations between these different entities.

Mr. Flores. Well, that sort of goes to my next question because we have talked a lot about how content is filtered online, but we need to consider how content is filtered through other platforms, even voice service devices. It has been reported that voice service devices prioritize certain content and services and they have even excluded certain products from their platforms.

So the first question is, are there anti-competitive concerns associated with this type of prioritization?

Mr. Pasquale. Congressman Flores, I have to confess I am not familiar with that niche of the market so I will have to pass.

Mr. Flores. Okay. That is fine. Let's move back to my initial question if we can. I would like to get the comments from the rest of the panel. Again the question was this. What are your thoughts as to whether policymakers need to establish a consistent legal and regulatory framework for how this data may be obtained and used? Let's start with Ms. Tucker.

Ms. Tucker. So I think it is very difficult -- and you have just told us this -- to have a consistent framework governing and technology. On the other hand, I think it is possible to identify areas where we are particularly concerned about privacy, be it health, be it kids, and make sure the policy is focused on protecting those outcomes we really care about.

Mr. Flores. Okay.

Dr. Ben-Shahar?

Mr. Ben-Shahar. My answer with all due respect is a resounding no. I don't think that policymakers should tell business what data to collect and how to use it.

Mr. Flores. In the interest of time I appreciate the short answer, okay.

Mr. Ben-Shahar. And maybe just set red lines.

Mr. Flores. Ms. Klonick, sorry.

Ms. Klonick. Yes. I think that regulation, Section 230 and any regulation that kind of curtails the ability of these businesses and platforms to self-regulate is probably not in the best interest of the public.

Mr. Flores. Okay, thank you.

And in the interest of time I will yield back the balance of my time.

Mr. Lance. Thank you very much. The chair recognizes Congresswoman Walters of California.

Mrs. Walters. Thank you. And thank you for holding this hearing and thanks to the witnesses for being here.

We can all agree that protecting consumers' information is paramount and that consumers deserve a clear understanding of their privacy expectations when using the internet. It is important we have this discussion so we can better understand how consumers benefit from current practice and examine ways to protect against those misuse of consumer information.

Professor Tucker, what is the best way to protect my constituents' privacy to make them feel secure and confident in the use of their data without impeding future innovation and America's leadership in the technology sector?

Ms. Tucker. So over the various sectors and various time periods, my research has repeatedly shown that the best way of introducing privacy protections is to give a sense of control back to consumers. Now that is distinct from transparency. It is distinct from disclosures. Instead, it is about restoring a sense of control. And what is more, my research has actually shown that that kind of policy is in from self-interest. And if you try and do the kind of microsegmentation using really personalized data, for example, preferences of someone over shoes, then those kind of, using that kind of data for advertising only works if there is a parallel sense of control among consumers.

Mrs. Walters. Okay, thank you.

Professor Ben-Shahar, what protections do existing legal schemes provide for consumers to protect them from the theft or loss of their data and are those legal schemes sufficient?

Mr. Ben-Shahar. Well, I think that again I am not a data security expert, but my understanding is that there are very few protections that are granted to consumers. Many of the things that were recommended that people do after, for example, the Equifax breach were fairly limited. I mentioned before in my testimony that I think that the reason there are so few remedies and recourses is because largely there is no evidence for the fact that consumers are suffering in a magnitude of harm that requires greater a remedy in this context.

Mrs. Walters. Okay. And then I have another question for you. How does the use of algorithms to deliver content impact consumers' experiences online and is there a benefit we see to the practice of collecting data?

Mr. Ben-Shahar. I think that benefit is enormous and it has been, you know, measured in many different ways. But I will just recommend to try one time to disconnect all the knowledge about you from your smart phone and see what happens. When you open Google Maps and want to go something and it no longer recognizes after the first letter where it is that you wanted to go and the inconvenience that you will say, ah, no, I wish the data service was still on, the recognition was on.

I think in many contexts personalization delivers astronomical value that has not yet been tapped. In my own research I am looking about at ways in which we can personalize legal rules and other things, but the only reason that we think about these new areas is because existing areas have proven to be enormously beneficial -- education, insurance, medicine, and the like.

Mrs. Walters. Okay, thank you.

And Professor Tucker, some digital platforms would say that when third parties are permitted to use their platform that platform gives consumers the tools to control their experience. Are we putting too much of the onus on the consumer to review the permissions the developer is requesting and forcing the consumer to choose which information to share?

Ms. Tucker. So I think this is a very good distinction to make in that, let's be clear, whenever we have actually studied search logs of how consumers behave when they are confronted by control, rather than opting out and, you know, protecting their privacy they tend to actually go in and try and improve the data, because there is nothing more irritating -- I don't know if this has happened to you that you are looking at a web service which thinks you are a 25 year old man and you are like, why do you think that? Consumers tend to try and improve the quality of data, intriguingly. The one distinction I do want to make though is that there are some categories of consumers where perhaps there isn't that level of control exerted. For example, we have a study right now which looks at apps which are targeted at toddlers. I don't know if you have ever been to a restaurant where parents are using these to quiet down their toddlers, but we saw that a vast quantity of data being collected. And there I think it is fair to assume that those toddlers are not really actually exerting any control on whether their location is being tracked or their use of the sort of My Little Pony app or whatever it is.

Mrs. Walters. Thank you and I yield back the balance of my time.

Mr. Lance. Thank you very much. The chair recognizes Congressman Costello.

Mr. Costello. Thank you. I want to share some reflections I have here and allow each of you to correct my understanding or enhance it, whatever terminology you may wish to use. From my perspective, browser history in some respects is a commodity but it is very invisible and at this point there is no regulatory framework for when and how it can be incorporated into an algorithm.

I take, and this is not a precise corollary, but if I made a phone call to you and the content of our discussion was transcribed and it was then sold or utilized for proprietary or commercial gain, there are some similarities between that and how an ISP is able to gather some of that content and then incorporate that into an algorithm or into how advertising would make its way into my internet searches, or if I go to a news website all of a sudden up pops laundry detergent if I was Googling laundry detergent.

Someone made the comment about editorializing content or raise concerns on the political side. It may have been Ms. Moy in her written testimony. I read everyone's written testimony. The trouble, the thing that I am grappling with on the concerns related to what kind of political content shows up and how you might be able to shape one's opinion of things is what is the difference between that and picking up a newspaper in the morning? And I don't really know how to distinguish between -- you can distinguish between the two, but in some respects I don't know that you should distinguish between the two.

As it relates to the Federal Trade Commission, if we are talking about particularly on political content, but even amongst other things, how would the FTC go about adjudicating equal time if we were to get into talking about political content and how does it get, how do you determine, oh, well, you put too much left-leaning or too much right-leaning content? I think that that can get deeply problematic.

And I believe, also, Ms. Moy mentioned something about adding protections for consumers, if you could share with me what kind of protections you might be speaking about.

The gentleman, I believe it was Dr. Ben-Shahar, I agree with your testimony. I don't think that these waivers or disclaimers or -- it doesn't mean a hill of beans. I totally agree with you. I am not sure, I think that is just more about indemnification or protecting one's liability and that is fine. I mean I don't think we should expect more from that. I don't know how you could expect more from it.

But the final thing I want to say for comment relates to Ms. Tucker's testimony. And in the final two paragraphs you talk about how different types of data can have different consequences and that any regulation, rather than treating all the data the same, needs to distinguish between what kinds of data may be actively harmful to consumers and what data may not be.

And it seems to me that we are really talking about values here, right. We want algorithms to be able to be helpful to the consumer and, candidly, in some respects helpful to those who are going to use that data to make sure that you have information that you may be more predisposed to wanting to see. We don't want that data to be harmful.

See, I am going on way too long. How do we create a clear yet evaluative standard and entrust everyone to follow it with enough tools for the FTC to embrace that kind of framework if we were to do it? I have spoke way too long. Comments?

Mr. Pasquale. I mean I just want to -- I have two quick responses, one being that I do think that, you know, in terms of thinking about what data is sensitive and what is not that can be a strength of a privacy regime.

But if we also look at the work on big data proxies, how like Nicholas Terry has described how you can have, say, location could be a proxy for race or the very data that you don't think is terribly sensitive could be a proxy for other data that is sensitive, that is where I would turn sort of Dr. Kearns' work against Dr. Tucker's work in a way and sort of say that there is a way in which, you know, it is because of these sort of inferences you can make from somewhat insensitive data to sensitive that is important.

With respect to Google and the newspaper, the difference that I would make is that I would say that what we are concerned often with respect to unfair algorithmic influence on political activity would be something that was a lot more subtle. So, for example, imagine if Facebook decided it was only going to encourage Democrats to vote. We do have studies that have shown that that can lead to I think it is a 0.63 or a small increase on the margin of the people whose feed is spiced with get out the vote advertisements.

So that is something I think we definitely have to look for because when a newspaper says vote for X, I can see that. But when Facebook, you know, suddenly spices the feed of the people that say it likes, then we can't see that.

Mr. Costello. Fair point.

Ms. Moy. So yes and I will just add, you know, when it comes to -- so a couple things. One, you know, when it comes to the FTC's enforcement authority, at the risk of sounding like a broken record the enforcement authority really is limited to deception, unfair and deceptive practices and there is no civil penalty authority.

But, you know, on your question of paid political ads, specifically, you know, I think that this is a really hard challenge that I suspect we don't have a lot of really good answers for yet on how to deal with. You know, one thing though is that there is very little transparency about what ads are being paid for and even when they contain political content. The FEC is conducting a rulemaking right now to at least explore the possibility of increasing transparency when it comes to labeling of political content on platforms, but -- or online I should say.

You know, but I think also this is a question where it might be extremely difficult to identify some political content, for example, when it relates to issues as opposed to candidates, without human eyeballs. And there is a tremendous amount of content that gets posted online and not nearly enough human eyeballs reviewing some of that content to determine whether and to what extent it might have a political effect.

Mr. Costello. I am just going to read this, something real quick into the record. I know you are ready to get out of here, Mr. Chairman. When someone states, quote, I could slow down -- well, we talked a lot about power that exists in the hands of those that are not ISPs. For instance, just last weekend, Matthew Prince, the CEO of Cloudflare, signaled he would look into taking up a challenge to slow down the FCC chairman's internet speed at his home. These apparently are not the least of the threats to Chairman Pai's home life. When someone states, quote, I could do this in a different but equally effective way -- and I would like to submit the entire string of tweets for the record -- isn't it clear there is a great deal of power in those that are not governed by the same rules in the internet ecosystem? And how would your reaction be different if an ISP did this rather than edge provider?

We don't have time, but if we could take any comments for the record on that because we are dealing with this larger net neutrality issue and I think some of the concerns are that it is not just ISPs that we should be looking at. There are some others that aren't governed that clearly have the power to do things that we all have concerns about. I yield back.

Mr. Lance. Thank you very much, Congressman Costello.

Seeing there are no further members wishing to ask questions, I thank all of our witnesses for being here today. Before we conclude, I include the following documents to be submitted for the record by unanimous consent: a paper from the 21st Century Privacy Coalition; a letter from the Electronic Privacy Information Center.

[The information follows:]

**********INSERT 8**********

Mr. Lance. Pursuant to committee rules, I remind members that they have 10 business days to submit additional questions for the record and I ask that witnesses submit their response within 10 business days upon receipt of the questions. Without objection, the subcommittee is adjourned.

[Whereupon, at 12:47 p.m., the subcommittee was adjourned.]