ACT | The App Association

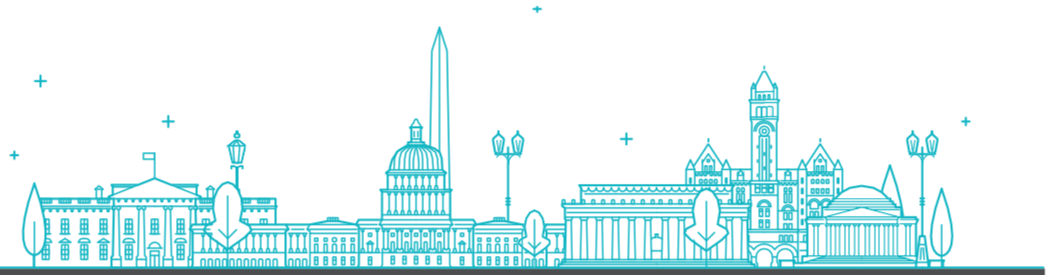
Protecting America’s Consumers: Bipartisan Legislation to Strengthen Data Privacy and Security

Testimony of

Graham Dufault
Senior Director for Public Policy
ACT | The App Association

Before the

U.S. House of Representatives
Committee on Energy and Commerce
Subcommittee on Consumer Protection and Commerce



1401 K Street NW Suite 501
Washington, DC 20005

☎ 202.331.2130
www. ACTonline.org

@ACTonline
/ACTonline.org

Executive Summary

ACT | The App Association (the App Association) is the leading trade group representing small mobile software and connected device companies in the app economy, a $6.3 trillion global ecosystem[1] led by U.S. companies and employing 205,360 people in Illinois and 237,090 in Florida.[2] Our member companies create the software that brings your smart devices to life. They also make the connected devices that are revolutionizing healthcare, education, public safety, and virtually all industry verticals. They propel the data-driven evolution of these industries and compete with each other and larger firms in a variety of ways, including on privacy and security protections.

We applaud this Subcommittee for its lead role in the 117th Congress' unprecedented progress toward a comprehensive federal privacy regime clarifying and enhancing the privacy and data security authorities of the Federal Trade Commission (FTC or Commission). Congress has never been closer to a compromise bill that would set a single, national set of rules for data privacy and security across all 50 states and the territories, while better protecting consumers and limiting unnecessary compliance costs and legal gamesmanship. We are especially pleased that Congress is taking meaningful steps toward a federal privacy framework, which policymakers should pursue to the exclusion of antitrust proposals that would manifestly weaken data privacy and security protections for your constituents.[3]

[1] ACT | THE APP ASSOCIATION, APP ECONOMY FAST FACTS (May 2022), *available at* *https://actonline.org/wp-content/uploads/About-the-App-Economy.pdf.*

[2] ACT | THE APP ASSOCIATION, STATE OF THE U.S. APP ECONOMY: 2020 (7th Ed.), *available at* https://actonline.org/wp-content/uploads/2020-App-economy-Report.pdf.

[3] *See* Letter from Morgan Reed, president, ACT | The App Association, to Majority Leader Chuck Schumer and Minority Leader Mitch McConnell, United States Senate, Re: Open App Markets Act (S. 2710) and American Innovation and Choice Online Act (S. 2992) Would Create Unacceptable New Threat Vectors in Mobile Ecosystems (Mar. 8, 2022).

Here is a summary of our takeaways regarding the draft American Data Privacy and Protection Act (ADPPA):

- **Preemption, Sec. 404(b)**
  - The overarching preemption language is reasonably strong, but a small tweak could enhance its effectiveness. Similarly, each exception to it could threaten its integrity and some of the exceptions would allow laws that fail to strike a reasonable balance to stand.

- **Private right of action, Sec. 403**
  - The right to sue for a violation of ADPPA is broad, applying to any person or class of persons, for an injury associated with a violation of ADPPA or regulations under it. It is also powerful, offering compensatory damages or injunctions as available remedies. However, we appreciate the guardrails in this draft, which we believe would help deter nuisance lawsuits and sue-and-settle business models that fail to benefit consumers while taxing small companies.

- **Small business treatment**
  - Although some of ADPPA’s provisions may be unnecessarily broad or subject covered entities and even consumers to undue risks, we believe the bill takes a balanced approach to small businesses, applying certain requirements only to large data holders and providing a safe harbor for small businesses under a certain threshold.

I. Preemption and Private Right of Action

A) Preemption, Sec. 404(b)

We have advocated for a federal privacy framework to include a preemption provision expressly preempting state laws for years now and appreciate that ADPPA includes one. The Information Technology and Innovation Foundation (ITIF) recently estimated the costs on businesses if 50 states enacted their own separate privacy regimes.[4] The study projected an annual cost of $98 to $112 billion for out-of-state companies, with $20 to $23 billion of that cost landing on small firms like App Association members. If we sound like a broken record on preemption, it is because these costs are avoidable and not necessary to meaningfully protect consumers from data privacy and security harms.

The overarching preemption language is reasonably strong, providing that no state or political subdivision of a state may "adopt, maintain, enforce, prescribe, or continue in effect" any law or provision having the force and effect of law, "covered by" the provisions of ADPPA or regulations promulgated under it. This construct should capture the general-applicability privacy laws that would create the most significant confusion, conflict, and compliance issues we have urged Congress to avoid as states enact slightly differing privacy requirements. However, we would recommend that the negotiators amend the provision to preempt any state provision "related to" the provisions of ADPPA. The Supreme Court has interpreted the "covered by" construct more narrowly than "related to," such that courts have upheld state laws directly regulating the subject of a federal law with "covered by" preemption language.[5] A strong, federal privacy law that comprehensively regulates data privacy and security activities should supersede state laws that address the same conduct, even if they have a narrower scope or more detailed requirements.

The 16 exceptions to the preemption provision make the "related to" construct especially important. Nonetheless, the negotiators should consider removing some of them because ADPPA is unlikely to preempt many of the laws the exceptions intend to address, so the exceptions may serve only to unintentionally except laws that should be preempted. Despite the established precedent on "related to" versus "covered by," courts have approached preemption of state laws in unpredictable ways, so we believe an express preemption provision is necessary to realize Congress' intent for a federal privacy framework to be the law of the land. Unfortunately, each exception creates additional risks that a court might expand its breadth to cover state laws and requirements that Congress never meant to except from preemption. For example, the exception for "laws that address health information" may be read to except a more general privacy law that happens to address health information not otherwise subject to

[4] INFO. TECH. & INNOVATION FOUNDATION, THE LOOMING COST OF A PATCHWORK OF STATE PRIVACY LAWS (Jan. 2022), *available at* https://cdn.sanity.io/files/03hnmfyj/production/2ecc8714efc329b2494f47cede821a40c9a0e6d5.pdf.

[5] *See CSX Transportation, Inc. v. Easterwood*, 507 U.S. 658, 664 (1993) (interpreting a "covered by" preemption clause); *Morales v. Trans World Airlines, Inc.*, 504 U.S. 374, 382 (1992) (interpreting a "relating to" preemption provision).

the Health Insurance Portability and Accountability Act (HIPAA)—a category of state requirement the bill probably intends to preempt. A broad reading of that exception, or another like it, might result in the state patchwork Congress seeks to avoid. ADPPA appropriately addresses healthcare data and subjects it to heightened requirements, including opt-in consent. As we noted in a letter to this Committee last year,[6] privacy abuses like the one at issue with the FTC's *Flo* settlement—which involved health data not otherwise covered by HIPAA—is one of the most important reasons for Congress to establish a federal privacy law.

Some of the specific laws that appear in the exceptions may also fail to strike the thoughtful balance the negotiators have in this draft.[7] We urge the negotiators to consider strengthening Sec. 404(b)(1) to preempt state provisions "related to" ADPPA's provisions and remove some of the exceptions in 404(b)(2)—or at least make one of those changes or the other. Arguably, many of those exceptions are unnecessary, especially if the negotiators keep the "covered by" language (which, all else equal, federal courts will likely interpret to let a broader class of state laws stand than if the provision used a "related to" construct).

Lastly, we agree with the bracketed text in Sec. 404(b)(2)(A), clarifying that a common law claim may not cite a violation of ADPPA as an element of liability. This language would help prevent private causes of action ADPPA does not intend to create in Sec. 403 or except from preemption in Sec. 404(b)(E).

B) Private Right of Action, Sec. 403

The negotiators have arrived at a reasonable compromise on this provision, which provides a good basis for further potential improvement. The private right of action (PRA) in ADPPA would apply to the entire Act and its regulations—except for data minimization, privacy by design, or data security requirements—and to any person or class injured by a violation. This provides especially broad coverage in terms of both which kinds of violations can give rise to a PRA and which categories of consumers may bring a PRA. For example, the PRA in this draft is available for almost all violations of the ADPPA and is not limited to a subset of injury types from a violation. Similarly, Sec. 404(b) prohibits pre-dispute arbitration agreements in certain circumstances (for example, with respect to individuals under the age of 18). Finally, the PRA in ADPPA would make powerful remedies available to individuals. In addition to compensatory damages, an individual litigant could seek and obtain an injunction for a violation of ADPPA or any of its regulations. The threat of an injunction can lead to much higher settlements because a putative defendant may be induced to pay an amount just under the cost of not being able to do business at all (e.g., the business's entire revenue amount for the duration of an injunction). As a corollary, injunctions can also be

[6] Letter from Morgan Reed, president, ACT | The App Association, to The Honorable Frank Pallone, Chairman, House Committee on Energy and Commerce, and The Honorable Cathy McMorris Rodgers, Republican Leader, House Committee on Energy and Commerce (Feb. 17, 2021).

[7] CLIFFORD CHANCE, THE COMING WAVE OF BIOMETRIC CLASS-ACTION SUITS, attorney advertising (Mar. 2021), *available at* https://www.cliffordchance.com/content/dam/cliffordchance/briefings/2021/03/The-Coming-Wave-of-Biometric-Class-Action-Suits.pdf.

attractive for opportunistic trial attorneys to engage in a pattern of suing and settling for frivolous reasons unrelated to protecting consumers because of their potentially higher payouts.

ADPPA's PRA includes a few safeguards that would mitigate the potential for the PRA to impose undue costs on covered entities, and we appreciate the negotiators' thoughtful approach in this regard. For example, before bringing a claim, an individual litigant would first have to notify the FTC and a state attorney general's (AG's) office, giving the enforcement agencies 60 days to determine whether to take on the complaint. If the agencies have declined to act on the complaint, then the individual or class may proceed with a demand letter to a target. Pursuant to Sec. 403(d), the demand letter must include a passage guiding the target to the FTC's website for further information, and pursuant to 403(c)(1) must also identify the specific provisions of the Act the target is alleged to have violated. Upon receipt of the demand letter, a small business target (or if an injunction is sought, any covered entity target) has a right to "cure" the alleged violation, "in the event a cure is possible." Under 403(c)(2), if the target "demonstrates it has cured the noticed violation or violations and provides the person . . . an express written statement that the violation or violations has been cured and that no further violations shall occur, an action for injunctive relief may be reasonably dismissed."

The safeguards here provide some meaningful protection from harassing and low-value lawsuits. However, we urge the negotiators to consider a few potential improvements. First, the PRA could be limited to a narrower subset of violations of the law. For example, a PRA may not be as helpful to remedy failures to respond to a request to correct but may be appropriate to address data security lapses (provided that the preemption exception for California's privacy law is removed). Second, the effect of the cure in 403(c)(2) may be unintentionally limited to providing for the reasonable dismissal of injunctions only, even if the target is a small business under 209(c). We believe this may be inadvertently narrow, given that 403(c)(1) provides a right to cure for injunctive relief *or* for presumably any relief sought against a small business under 209(c). We recommend the negotiators amend 403(c)(2) to read (new text in bold), "an action for injunctive relief **or, with respect to an action against a covered entity that meets the requirements of section 209(c) of this Act, an action for any relief provided in section 403(a)(2),** ~~may be reasonably dismissed~~ **shall not be permitted and may be reasonably dismissed**." Without a change along these lines, the legislation might unintentionally limit the effect of a cure for small businesses—and adding "shall not be permitted" could strengthen the provision and give courts more cover for dismissal. Third, we urge the negotiators to consider limiting the PRA to a subset of injury types. For example, instead of any injury giving rise to a PRA, it could be limited to "substantial" privacy harms resulting from a given violation, providing a more meaningful deterrent to lawsuits that impose disproportionate costs on small companies for relatively minor issues. Lastly, negotiators could require private litigants to show that covered entities possessed some level of scienter (or consciousness) of the alleged violation. This additional safeguard would help protect small businesses from facing private lawsuits involving good faith or inadvertent lapses that result in little or no harm to individuals.

II. Consumer and Civil Rights

One of our primary asks of Congress has been for a federal privacy bill to include a set of consumer rights, "implemented in a way that avoids additional compliance layers without enhancing consumer understanding and trust."[8] The balance the negotiators struck with ADPPA is a solid foundation. However, we have some constructive feedback for the negotiators to consider as they continue their work.

A) Consumer Rights, Sec. 202

Sec. 202(b)(9) would require covered entities to disclose "whether or not any covered data collected by the covered entity is transferred to, processed in, or otherwise made available to" China, Russia, Iran, or North Korea. We share the concerns with foreign adversaries' access to and exploitation of Americans' data. Even so, the location of data may provide less valuable insights into the risk than whether foreign adversaries are able to access it. For example, if a company is based in such a country—and therefore subject to the adversary's national security and surveillance laws—then even if the data is stored outside that country, we should worry about its access to Americans' data stored by that company. Meanwhile, an American app company may be barred under U.S. law from cooperating with foreign adversary investigators, illustrating that the location of the data alone is instructive but not as dispositive of a foreign adversary's access to it than whether the company is based in that country. There do not appear to be any restrictions on the app company from caveating the 202(b)(9) disclosure to accurately reflect why it may need to process data in China or another of those countries—and therefore clarify that such processing should present no additional risk to Americans. Clarifying this in the bill or report language may help ameliorate any unintended consequences of the provision.

B) Civil Rights, Sec. 207

This section includes a requirement for covered entities to conduct either an "impact assessment" (if they are large data holders) or an "algorithm design evaluation" if a non-large data holder develops the algorithm itself. We urge the negotiators to consider couple of factors on these provisions. First, the impact assessment provision applying to large data holders might inadequately protect sensitive information related to the algorithm, its training, and its use. Sec. 207(c)(3)(C)(ii) allows the covered entity to redact "trade secrets," but there may be other information that, if it lands in the wrong hands, may pose unintended consequences. Similarly, the requirement to allow access to any Member of Congress may inadvertently result in sensitive non-public information being published or placed in the hands of an entity that may seek to harm the individuals to which it pertains. Accordingly, we encourage the negotiators to reconsider allowing such access to any congressional office and to impose safeguards on access to impact assessments in the hands of the FTC (e.g., by providing an exemption from

[8] *See* ACT | THE APP ASSOCIATION, PROTECTING CONSUMER PRIVACY GROWS SMALL BUSINESS (May 2022), *available at* https://actonline.org/wp-content/uploads/Protecting-Consumer-Privacy-Grows-Small-Business95-1.pdf.

the Freedom of Information Act (FOIA)). Second, we urge the negotiators to consider amending Sec. 207(c)(3)(B) so that it reads "to the extent practicable" instead of "possible." Hiring an external firm to evaluate an algorithm may impose costs on small firms developing lower-risk algorithms that are not justified by the benefits. Accordingly, we also urge the negotiators to amend 207(b)(5)(B) so that it reads "shall exclude" instead of "may exclude." This change would appropriately require the FTC to exclude low and minimal risk algorithms from the requirements' coverage, instead of leaving it to the agency's discretion.

We appreciate that this provision appropriately scopes the role of the FTC to one in which the agency assists other agencies in enforcing other existing civil rights laws, where applicable. We have urged this approach in the past and appreciate that the negotiators have adopted it with the ADPPA draft. However, the PRA also applies to this section, so individuals may sue for a violation of it. Sec. 207(a)(1) would broadly prohibit collecting, processing, or transferring covered data in a manner that "discriminates or otherwise makes unavailable the equal enjoyment of goods or services on the basis of race, color, religion, national origin, gender, sexual orientation, or disability." Since other laws address these forms of discrimination (although perhaps not explicitly as it relates to transferring or processing data in a manner that results in discrimination), it is unclear to what extent a PRA for such discrimination would be duplicative of those other civil rights laws. Protecting civil rights is rightfully a priority for the negotiators, but we urge caution as to how opportunistic litigants may widen or contort a broad prohibition like the one in 207(a)(1). For example, the Virginia Consumer Privacy Act and the Connecticut consumer privacy law both prohibit processing personal data in violation of state and federal laws that prohibit unlawful discrimination against consumers.[9] This approach could more directly address the problem without inadvertently broadening liability beyond its intended scope. We look forward to working with the negotiators to better understand how they intend for it to be enforced.

[9] *See* Va. Code Ann. 59.1-571 – 59.1-581 (2021); Connecticut State Senate, Substitute Senate Bill No. 6, Pub. Act No. 22-15 (2022 Sess.), *available at* https://www.cga.ct.gov/2022/ACT/PA/PDF/2022PA-00015-R00SB-00006-PA.PDF.

III. Definitions

A) Sensitive covered data, Sec. 2(22)

ADPPA requires covered entities to obtain express, affirmative consent for collecting and processing sensitive covered data, so the definition should not extend to substantially all data. There are a few categories of data that we urge the negotiators to consider removing from the definition of sensitive covered data:

- Sec. 2(22)(i) – This provision appropriately includes Social Security numbers (SSNs), other government identification, etc., but the exception for "required by law" to be displayed may be narrow. This exception should be broadened to include such information that is "lawfully made available publicly," or a similar construct that would remove publicly available government identification information from sensitive covered data.
- Sec. 2(22)(vii) – This provision appropriately includes the content of certain personal communications, but also certain metadata associated with those communications. We believe it may be unnecessary to include "any information that pertains to the transmission of voice communications," as it could sweep in more metadata than the provision intends.
- Sec. 2(22)(xii) – This provision includes "calendar information" and related pieces of information. This may unintentionally add unnecessary friction where, for example, an app seeks to add or export an event to or from a separate app, and we urge the negotiators to remove it.
- Sec. 2(22)(xiv) – This provision covers viewing habits. It may also unintentionally add friction where a consumer intends to provide access to their streaming viewing information in the course of using a streaming service.

B) Biometric Information, Sec. 2(3)

The definition of "biometric information" in ADPPA includes "facial or hand imagery," which are broad concepts that may sweep in more than the negotiators intend. For example, modern smart devices often use this kind of imagery to authenticate users each time they want to access their device or an app. Requiring opt-in consent for each use could in many cases add needless friction for authentication uses, even if more sensitive uses (such as one-to-many identification) might generally warrant opt-in consent.

C) Covered Data, Sec. 2(8)

The definition is a thoughtful one that appropriately excludes de-identified data, employee data, and publicly available information and we appreciate that ADPPA endorses a privacy by design approach. However, we urge the negotiators to consider whether the draft could clarify that when a covered entity designs secure systems that put data in control of the user in a manner that shields it from the covered entity's access, the draft avoids unnecessarily subjecting such data to opt-in consent and other requirements.

IV. Other Provisions

A) Data minimization, Sec. 101

We applaud the negotiators for adopting a workable data minimization framework. The provision would prohibit collections, processing, or transfer beyond what is reasonably necessary, proportionate, and limited to products and services requested by the individual or communications anticipated within the context of the relationship. We had advocated for negotiators to avoid the approach of barring all processing unless a lawful basis exists and ADPPA's framework fortunately takes the more flexible approach. We also appreciate that instead of rules, ADPPA requires the FTC to issue nonbinding guidance, which will help inform covered entities without subjecting them to more complex forms of liability.

B) Data protections for children and minors, Sec. 205

We welcome provisions to strengthen privacy protections for children and adolescents beyond the Children's Online Privacy Protection Act (COPPA). We appreciate the goals of the negotiators in addressing targeted advertising to minors and agree that Congress should address the issue. However, we note that there may be constitutional implications for an outright ban on certain kinds of advertising. Experience has shown that bans on advertising, even to minors, have had difficulty standing up to First Amendment scrutiny,[10] and there may be less constitutionally fraught ways of dealing with the issues the negotiators seek to address. We would welcome the opportunity to work with the negotiators on this provision.

We also appreciate that Sec. 205(d) would require the FTC's Inspector General to issue a report on COPPA's safe harbors. The safe harbor program plays a vital role in enabling small businesses to appropriately protect kids online and helps send a signal to parents that an appropriate third party has reviewed and certified an app or other service's compliance. This Subcommittee's rigorous oversight could help strengthen and improve the program and we welcome this scrutiny.

C) Small business provisions, Secs. 209(c), 304

Sec. 304 appropriately provides a safe harbor for small businesses adhering to compliance programs that "meet or exceed" the ADPPA's requirements, with a reasonable threshold described at 209(c). Notably, 209(c)'s threshold is pegged at $41 million in annual revenue or processing data on 100,000 or fewer *individuals*—as opposed to devices—per year on average over the most recent three-year period. We appreciate the negotiators' recognition that the number of connected devices per household has doubled over the past few years and therefore a threshold based on number of devices may be a less accurate reflection of the breadth of a company's impact on consumers. The safe harbor would ensure that App Association members are

[10] *See Reno v. ACLU*, 521 U.S. 844 (1997).

rightfully viewed as—and held accountable for—complying with a federal framework, while alleviating liability concerns and compliance burdens.

V. Oppose Antitrust Proposals That Prohibit Privacy and Security

Pending legislation in both chambers—the American Innovation and Choice Online Act (S. 2992/H.R. 3816) and the Open App Markets Act (S. 2710/H.R. 7030)—would prohibit key privacy and security measures that protect consumers on their mobile devices. For example, mobile software platforms (app store / operating system combinations) recently introduced additional controls for smartphone owners, enabling them to limit the ability for one app to track their activities across other apps. Apple's version of the feature is called AppTrackingTransparency (ATT), which has been available for about a year[11]—and Android's, called Privacy Sandbox, was announced in February.[12]

Controls like ATT and Privacy Sandbox address a notoriously intractable information asymmetry problem with online services—that the behavioral advertisers building profiles on people know a lot more about what they're doing than consumers themselves. The information asymmetry problem is a common form of "market failure," if it leads to consumers not understanding an economic bargain and therefore may distort the market. But in this case, the market itself has produced solutions that consumers seem to use, as statistics indicate that 75 to 90 percent of consumers[13] are opting out of cross-app tracking. ATT and Privacy Sandbox are a good start, but we still need a federal privacy law. Controls like this should be available in other marketplaces, not just on smartphones. H.R. 3816 and H.R. 7030 would essentially prohibit ATT and Privacy Sandbox, so we urge members of this Subcommittee to oppose the bills for the same reasons as supporting privacy legislation.

Certainly, free online services and ad-supported apps are important options. Some of our member companies offer ad-supported apps and many of them benefit from knowing whether an ad they've purchased was successful. However, an ecosystem in which that overarching model is the *only* choice—and that unshackles abuses in data collection—obviously fails to serve most consumers, at least the large majority who have opted out of cross-app tracking. And advertising is not valueless, nor is it inherently less effective, with the introduction of more effective consent mechanisms. Of course, the corollary to the notion that consumers care about privacy is that they are

[11] Anthony Ha, "Apple's App Tracking Transparency feature has arrived – here's what you need to know," TECHCRUNCH (Apr. 26, 2021), *available at* https://techcrunch.com/2021/04/26/apples-app-tracking-transparency-feature-has-arrived-heres-what-you-need-to-know/.

[12] Anthony Chavez, VP, Product Management, Android Security & Privacy, "Introducing the Privacy Sandbox on Android," The Keyword blog (Feb. 16, 2022), *available at* https://blog.google/products/android/introducing-privacy-sandbox-android/.

[13] Manoj Balasubramanian, "App Tracking Transparency Opt-In Rate – Monthly Updates," Flurry (May 2, 2022), *available at* https://www.flurry.com/blog/att-opt-in-rate-monthly-updates/.

willing to pay for it. For example, one white paper found a 0.3 percent increase[14] in the likelihood that an iOS app would be paid or offer in-app payments after Apple rolled out ATT. Even so, the fact that this effect is infinitesimal pokes a hole in inflated rhetoric around ATT's competition foreclosure effects, and it also suggests the direct costs of privacy controls are, thus far, insubstantial (even if consumers *are* willing to pay more for privacy).

If Congress wants to improve the competitive prospects of nascent and smaller competitors in the app economy, diminishing the value of the app stores by steamrolling their privacy features is not a welcome solution. Rather, we believe this Subcommittee's and its counterparts' work on ADPPA and similar measures could uplift the value of all the other distribution options, including the open internet, by subjecting the broader ecosystem to a set of national requirements. That way, consumers think about digital goods and services as privacy protective whether they are obtained through a mobile software platform or on an HTML website. We would prefer the route of enhancing the value of all the competitive alternatives rather than destroying one of them.

VI. Conclusion

As a key negotiator in the bicameral, bipartisan effort to enact federal privacy reform, this Subcommittee's work must be commended, and we hope our input is a constructive addition to the negotiators' work. We look forward to further assisting these efforts as the process unfolds.

[14] Reinhold Kesler, "The Impact of Apple's App Tracking Transparency on App Monetization," Work in Progress (Apr. 14, 2022), *available at* https://www.dropbox.com/s/miom2cdoub8241w/ATT_Paper_Kesler.pdf?dl=0.

Appendix: App Economy Innovators in Your Districts

Tech driven small businesses are the backbone of innovation, driving solutions that power how we live, work, and play through safe, secure, connected technology. Below you will find companies in corresponding congressional districts for each member of the Subcommittee on Consumer Protection and Commerce. These companies are not only driving innovation across the app economy, but they're also creating jobs and opportunities in your communities, taking your district, and our nation, further into the 21st century workforce as global leaders.

Majority

Rep. Jan Schakowsky, Chair (IL-09)
Company: Kidz Learn Applications

The one-woman team at Kidz Learn Applications has been developing iOS and Android mobile apps that provide educational content to children for the past decade. Kidz Learn Applications has developed more than 20 apps with lessons ranging from math to vocabulary and even created a guide for educational, kid-friendly places in New York City for a day of fun for kids and adults alike.

Rep. Bobby Rush (IL-01)
Company: Duality Accelerator

Founded just last year, Duality Accelerator is a 12-month program based in Chicago that helps early-stage software and hardware startups to reach a viable stage of business. Their first cohort consisted of six companies engaging in quantum technology, and they have partnered with entities such as the Universities of Illinois and Chicago as well as Argonne National Laboratory and the Chicago Quantum Exchange.

Rep. Kathy Castor (FL-14)
Company: Accusoft

Located in Tampa with 170 employees, Accusoft, originally founded as Pegasus Imaging Corporation in 1991, focuses primarily on content processing through image and document cleanup while providing application programming interfaces (APIs) and barcode collection through mobile apps. They also provide digital conversion tools that turn paper document and paper-based processes (often found in legal, financial, and health transactions) into customized digital processes based on each client's unique needs.

Rep. Lori Trahan (MA-03)
Company: Fisheye Software

Founded in 1997 and located in Maynard, Fisheye Software focuses on building enterprise-level software that makes complex systems easier to understand. They provide services to a number of clients, both in the government and commercial systems, contributing to anything from data archiving to air traffic control or missile defense systems.

Rep. Jerry McNerney (CA-09)
Company: CloudKrest Technology Solutions

Cloudkrest is a two-person digital marketing solutions company located in Stockton and has been in business since 2017. Cloudkrest is focused specifically on web design, app development, digital branding, and content creation with customers both local and international.

Rep. Yvette Clarke (NY-09)
Company: Stellar Health

Since Stellar Health's founding in 2018, this Manhattan-based healthcare technology company has rapidly grown to nearly 200 employees and is providing connected health solutions to patients everywhere. Stellar Health helps provide providers with targeted recommendations to deliver value-based improvements to care and financial performance to hospitals. This means that through Stellar Health's services, patients receive care faster and at a lower cost throughout the care chain.

Rep. Tony Cárdenas (CA-29)
Company: Swift 200

Located in Panorama City, Swift 200 is a custom software development firm that works to solve a wide range of problems for clients of varying sizes within the app economy. From content marketing and search engine optimization (SEO) to web and mobile application development, Swift takes projects from idea to reality.

Rep. Debbie Dingell (MI-12)
Company: Arbormoon Software Inc.

Founded in 2004, the eight-person team at Arbormoon Software focuses almost entirely on mobile app development, whether it be iOS or Android. Based in Ann Arbor, they have created apps for the University of Michigan as well as SiriusXM, Peterbilt, local radio stations, and a number of other small businesses and startups local to the area.

Rep. Robin Kelly (IL-02)
Company: Pathfinder

Based in Kankakee and founded in 2020, Pathfinder is a full-service creative marketing agency that helps their clients tell stories through web and mobile solutions. Having grown to nearly 100 employees in less than two years, their offerings include web development, graphic design, photography, and other digital marketing offerings.

Rep. Darren Soto (FL-09)
Company: Yac

Originally founded as “Yelling Across Cubicles”—because it was essentially built as a digital walkie talkie to be used in the workplace—Yac was founded in 2019 and located in Kissimmee. Since then, Yac has grown to include other functionality including asynchronous meetings, voice messages, screensharing, and shareable links, all focused on making remote work more collaborative.

Rep. Kathleen Rice (NY-04)
Company: AppSoft Technologies, Inc.

Located in Garden City and founded in 2015, AppSoft Technologies creates mobile applications for entertainment and gaming audiences. AppSoft Technology is singularly focused on creating mobile apps that are geared towards video games, esports news, and information. They also acquire existing games and redevelop or otherwise improve them.

Rep. Angie Craig (MN-02)
Company: Avionte Staffing and Recruiting Software

Avionte Staffing and Recruiting Software, located in Eagan, provides solutions for payroll, attendance, and billing, as well as customer relationship management, new job applications, and onboarding capabilities. Since opening their doors in 2005, they have served more than 900 customers and nearly 25,000 users across the United States and Canada.

Rep. Lizzie Fletcher (TX-07)
Company: For All Abilities

For All Abilities is a software platform that helps companies address and provide for their employees with disabilities. The platform assesses employees and then prescribes and trains them to use individualizes supports and accommodations that meet ADA requirements.

Rep. Frank Pallone, *Ex officio* (NJ-06)
Company: DealerApp Vantage

DealerApp Vantage, located in Piscataway, is the nation’s leading native mobile app development company that specializes in automotive dealers. They have mobile app solutions aimed to fit all budgets and sizes, from small business, single roof top dealerships to some of the largest auto groups in the United States.

Minority

Rep. Gus Bilirakis, Ranking Member (FL-12)
Company: Thinkamingo

Since 2011, Tampa-based Thinkamingo has been a husband-and-wife team working together to build family friendly, education-focused mobile apps. Their apps range from interactive dice meant to take young writers to inspired story tellers to imagination-driven spy kits complete with virtual disguises, including a voice changer.

Rep. Fred Upton (MI-06)
Company: SPARK Business Works
Founded nearly five years ago and headquartered in Kalamazoo, with two other offices in the state, SPARK Business Works is a custom software development and design firm. They stand prepared to help businesses of any size create an effective online presence that aims to improve each client's unique needs for the connected customer experience.

Rep. Bob Latta (OH-05)
Company: Spoke Design LLC
Spoke Design helps businesses of all sizes build their brand and digital presence through their full-service design and web agency. Founded 13 years ago in Toledo, Spoke offers full-stack development as well as thoughtful user experience and interface design.

Rep. Brett Guthrie (KY-02)
Company: BEHAVR
Founded in 2016, BEHAVR is creatively utilizing virtual reality technology to help revolutionize the way that people handle anxiety-related disorders. Based in Elizabethtown with a team of over 50 employees, BEHAVR helps treat stress, fear, and anxiety through the use of gradual exposure to the situations that provoke the negative emotions.

Rep. Larry Bucshon (IN-08)
Company: Gropod
Located in Evansville and founded in 2016, Gropod is working to help people grow their own food through technology in order to create a more sustainable world and allow people to increase their food independence. With 12 employees, Gropod is building hydroponic farming systems that can grow anything from lettuce and other vegetables to any number of fruits or spices.

Rep. Neal Dunn (FL-02)
Company: TechFarms
TechFarms, founded in 2015 and located in Panama City Beach, has a singular mission: create a more technology-focused and vibrant entrepreneurial ecosystem in northwestern Florida. The team at TechFarms has created a collaborative coworking space for local business owners with the goal of lifting up the whole community.

Rep. Debbie Lesko (AZ-08)
Company: No Boundaries Marketing Group
The 10-person team at No Boundaries Marketing Group works to simplify digital marketing and advertising for small to medium-sized businesses. They were founded in Surprise in 2019 and provide search engine optimization (SEO) as well as other strategic, digital, and traditional marketing services.

Rep. Greg Pence (IN-06)
Company: Accutech Systems Corporation
Located in Muncie and founded in 1987, Accutech provides software solutions and services to those in the financial industry. Accutech's solutions include a wealth management platform and mobile applications that make opening an account easy, as well as a business intelligence dashboard.

Rep. Kelly Armstrong (ND-AL)
Company: Bushel
Located in Fargo and founded in 2017, Bushel leverages technology to help serve participants in the grain industry through mobile applications, websites, and other elements of digital infrastructure. Bushel provides a number of solutions and products that aim to help those in the grain industry create a more streamlined workflow.

Rep. Cathy McMorris Rodgers, *Ex officio* (WA-05)
Company: Gestalt
Founded in 2017, Gestalt is a 15-person team working to bring healthcare into the 21st century by replacing microscopes and glass slides with automated, electronic, and digital workflows. They provide services related to pathology in the medical field to professionals as well as those in education or academic research.