ACT | The App Association

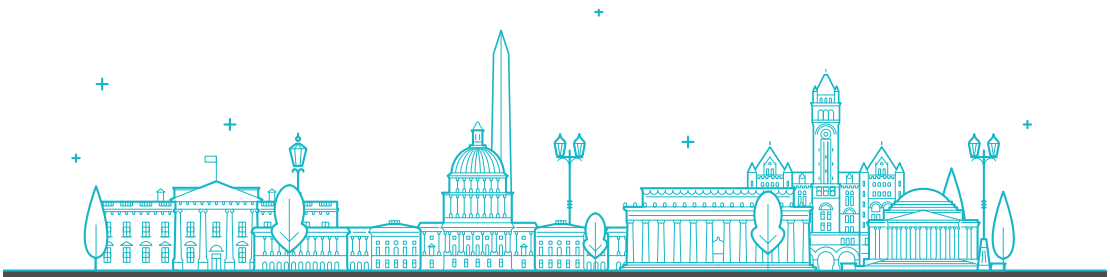
Protecting Consumer Privacy

Testimony of

Morgan Reed
President
ACT | The App Association

Before the

U.S. Senate
Committee on Commerce, Science, & Transportation



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 $1.7 trillion ecosystem employing 186,590 people in Washington and 14,190 in Mississippi.[1] 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.

One of the foundational imperatives for the success of small business innovators in the app economy is consumer trust in the marketplace. The vast majority of mobile device users cite trust as the number one factor when deciding to grant an app access to their personal data, and users already commonly restrict access and delete apps they believe pose a privacy risk.[2] Eighty-nine percent of users have at some point denied features, such as microphone or location access, to an app they did not trust, while 63 percent of users have deleted an app outright due to privacy concerns.[3] Because our member companies are small and often young companies, they rely more heavily on the privacy and security protections and controls that protect consumers from bad actors than their larger, more established counterparts—which depend more on brand name reputation and recognition. Therefore, the Committee's and the Federal Trade Commission's (FTC's) role in holding bad actors accountable is critical to the success of App Association members. Specifically, we urge you to take the following recommendations into account as you evaluate next steps on consumer privacy:

1. **Congress Should Guide FTC Enforcement Authority and Resources.** Though the FTC is the main privacy enforcer at the federal level and has its hands full in recent years with the proliferation of privacy, security, and other consumer protection issues, it often lacks the statutory authority and/or dedicated funding to carry out its mission to the fullest potential.

2. **Congress Should Avoid Forcing the FTC to Stretch its Own Authority.** The FTC's recent steps to bolster its leadership in the privacy space, while certainly understandable, demonstrate that the Commission is working with limited tools at its disposal.

3. **Congress Should Enact a Federal Privacy Framework.** The single most impactful policy decision Congress can make to combat existing and future privacy harms is to enact comprehensive privacy legislation that grants strong consumer rights to the citizens of all 50 states simultaneously.

4. **Congress Should Avoid Antitrust Measures that Presume the Illegality of Platform-Level Privacy Protections.** These proposals could unintentionally render widely-adopted privacy protections illegal, especially those that consumers use on their smart devices, exposing consumer data to greater privacy and security risks.

---

[1] 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.

[2] 14. DELOITTE, TRUST: IS THERE AN APP FOR THAT? DELOITTE AUSTRALIAN PRIVACY INDEX 2019, (2019), *available at* https://www2.deloitte.com/content/dam/Deloitte/au/Documents/risk/deloitte-au-risk-privacy-index-150519.pdf.

[3] *Id.* at 6

We deeply appreciate your leadership as the Senate Commerce Committee continues to navigate the unprecedented COVID-19 pandemic and works to get our economy back on track. As part of these efforts, we ask that you continue the bipartisan work of crafting a single set of rules governing the privacy practices of entities that generally fall under the FTC's jurisdiction. Recent events and the forced shift of daily and essential activities—including core healthcare and communication services—to the digital space has underscored the need for Congress to act decisively on this issue.

I. Congress Should Guide FTC Enforcement Authority and Resources

We support enhancing the enforcement capabilities and resources for the FTC to stop and prevent consumer protection harms by bad actors. The FTC needs more appropriate tools with Congress' direction to stop consumer harms resulting from privacy and data security abuses in particular, as those problems have proliferated and continue to generate headlines and stoke constituent outrage.

Recent activity in the House Energy & Commerce Committee indicates that lawmakers are seriously mulling increased funding for the FTC as part of ongoing deliberations on the budget reconciliation package. In particular, the House Energy & Commerce Committee voted to approve $1 billion in additional appropriations for the Commission to establish new a privacy bureau to conduct work "related to unfair or deceptive acts or practices relating to privacy, data security, identity theft, data abuses, and related matters."[4] In general, App Association members support vigorous management of the marketplace for bad actors, especially those that circumvent rules in a way that reduces overall trust in the app ecosystem or that threaten an even playing field in the marketplace. However, in this case, we believe that Congress should not act in half measures on privacy and that empowering the FTC with augmented capabilities to address privacy harms should take the form of a comprehensive federal privacy regime. Simply establishing a new bureau with additional resources does little to enhance enforcement remedies, nor does it more clearly delineate the breadth and boundaries of the FTC's authority on privacy practices.

We also appreciate and understand the intent behind proposals originating in the House Energy & Commerce Committee to bolster the FTC's enforcement authority. At the same time, we continue to have concerns with granting the Commission, or any new regulatory body, general, *undirected* rulemaking authority to regulate privacy harms. The same concerns extend to even more general rulemaking authority to regulate *all* consumer protection harms under the FTC's purview. As we've previously written, we recommend providing only narrow rulemaking authority on the issue of privacy, as "[t]he swath of the economy and range of economic activities" any privacy regulator would oversee is "too broad for it to promulgate generally applicable rules that successfully balance the finer conflicts of purpose in the many sectors that would be subject to those requirements."[5] A general grant of rulemaking authority to define unfair or deceptive acts or practices in or affecting commerce would completely delegate the exercise of defining limits to the Commission's own powers to the agency itself—a task better suited to Congress. A Democratic Congress imposed additional procedural

[4] *See* Committee Print by the Committee on Energy and Commerce, Title III, Subtitle O, §31501, *available at* https://privacyblogfullservice.huntonwilliamsblogs.com/wp-content/uploads/sites/28/2021/09/BILLS-117pih-SubtitleO.pdf

[5] Letter from Graham Dufault and Madeline Zick to the Honorable Anna Eshoo and the Honorable Zoe Lofgren, Members of Congress, re: Draft Framework of Online Privacy Act of 2019 (Jul. 18, 2019).

hurdles on the Commission's rulemaking authority in 1980[6] for just this reason. The sheer breadth of its purview was better adapted for an adjudicative approach and invited overreach with rulemaking.

Aside from potential overreach and its relative unsuitability in regulating the dynamic markets the FTC oversees, general rulemaking also creates substantial uncertainty and potential instability. For example, an FTC controlled by one party might construct a carefully segmented regulatory regime, categorizing consumer protection harms by industry. The next Administration might have a completely different regulatory philosophy and scrap the framework entirely. Without guardrails in statute, challenges to such a complete deletion of regulations might fail—according to jurisprudence evaluating federal agency decision-making, the courts grant "*Chevron* deference" to those interpretations.[7] The less there is for an agency to interpret, the more leeway an agency has to define its own goals and decisions.[8] The result could be massive swings in consumer protection regulation from one agency to the next (mainly unchecked by the courts), and in all likelihood, a more purposeful focus on political aims and headlines rather than targeting practices that are net harmful to consumers. Even where Congress has explicitly outlined regulatory goals and purposes, shifts in Administration have brought uncertainty, especially to more dynamic markets. The effect could be much worse without clear statutory guidance on the limits and purposes of FTC rules and enforcement.

As Rob Coons, chief revenue officer of App Association member Walker Tracker—a platform for people to compete with each other on step challenges and similar wellness activities—points out, regulatory uncertainty falls heavily on small companies like his. For example, as states and governments overseas recently enacted new and differing general consumer privacy laws, Walker Tracker went back to the drawing board on its data processing agreements with employer clients. In turn, Walker Tracker now turns down contracts under a certain dollar threshold with smaller companies because the costs of uncertainty are too high to justify working on smaller contracts. Further privacy shifts at the state level coupled with regulatory pirouetting at the federal level would only worsen the situation for Walker Tracker and other App Association members.

We have similar concerns with granting the Commission broad civil penalty authority for any violation of the FTC Act, as legislation pending in the House would do. Although we support granting the Commission civil penalty authority for specific kinds of offenses, including as part of a general privacy bill, civil penalties for cases of first impression would chill innovation that has a net positive effect on consumer welfare. For example, when the Commission first encountered social media influencers, it quickly developed guidance outlining proper disclosures for influencers who receive compensation for endorsing products and services.[9] A fast-developing business that blurred the lines between personal networking and advertising, "influencing" cried out for FTC clarity on when it crosses the line into deception. If the FTC had civil penalty authority—providing up to $44,000 per violation—in cases where market participants have little notice as to where the line is for social media influencing, the cost of those potential penalties might have discouraged the practice altogether. Although influencing may have gained an unserious reputation,[10] its emergence created legitimate livelihoods where none previously existed. And while authorizing civil penalties for first offenses—under the broad

---

[6] *See* the Federal Trade Commission Improvements Act of 1980 (H.R. 2313, 96th Cong.).
[7] *See Chevron U.S.A., Inc. v. Natural Resources Defense Council, Inc.*, 467 U.S. 837 (1984); *Astrue v. Capato*, 566 U.S. 541 (2012).
[8] *Id.*
[9] DISCLOSURES 101 FOR SOCIAL MEDIA INFLUENCERS, FED. TRADE COMM'N (Nov. 2019), *available at* https://www.ftc.gov/system/files/documents/plain-language/1001a-influencer-guide-508_1.pdf.
[10] Influencers in the Wild, @influencersinthewild, INSTAGRAM, https://www.instagram.com/influencersinthewild/?hl=en (last visited Jul. 25, 2021).

prohibitions in Section 5—would not necessarily cause the FTC to shoot first and ask questions later, it certainly could allow for such an enforcement approach.

The risk of such a regime falls especially heavily on small companies like App Association members. Marc Fischer, chief executive officer of App Association member Dogtown Media, says the prospect of civil penalties in undefined cases could cause longer timelines for product and service development and higher insurance costs. Dogtown Media is a mobile media development firm that has created more than 200 apps on behalf of clients in a wide variety of industries, and like many of its peers, buys business risk insurance. As Marc points out, those costs would likely increase with the prospect of monetary penalties for first-time offenses, and the additional money he spends on those premiums should instead go toward hiring and business development.

The concerns are especially acute where companies, like Dogtown Media, are forging cutting edge uses for advanced technologies like artificial intelligence (AI). Publicly traded firms with high-powered attorneys may be able to pay heavy fines and move on, but those penalties could deal a devastating financial blow to small companies like App Association members.

Other reform proposals on the House side that would enhance the FTC's authority cause similar concerns for our member companies, although we would support these limited expansions in some forms in the context of a general privacy bill. For example, possible reforms could expand the FTC's jurisdiction to cover non-profit entities or expand FTC jurisdiction to cover common carriers under the Communications Act (telecommunications and wireless carriers, for example). It may make sense to enable the FTC to cover these kinds of entities in a more limited context like a general privacy bill, but we would be concerned about adding breadth to the FTC's purview generally. For Communications Act common carriers and non-profit entities, we have seen provisions in privacy bills that would place both categories into FTC jurisdiction—while carving those common carriers out of Communications Act jurisdiction—for the purposes of the privacy law and regulations promulgated under it.[11] The FTC is a more experienced privacy enforcer than the Federal Communications Commission (FCC), so it makes sense to task the FTC with monitoring privacy practices of wireless carriers instead of the FCC. The targeted treatment of telecommunications common carriers also avoids overlapping regulation of certain entities by multiple federal agencies. App Association members demand high quality services at the lowest possible costs from internet service providers and understand that subjecting them to duplicative regulatory compliance and penalties from multiple federal agencies could increase costs and diminish service quality.

II. Congress Should Avoid Forcing the FTC to Stretch Its Own Authority

Absent action from Congress to grant additional rulemaking authorities to the Commission, either through a comprehensive privacy law or otherwise, the Commission is likely to take it upon itself to reinterpret its existing authorities to better police the marketplace. While certainly an understandable impulse in the face of a rapidly evolving digital ecosystem and host of novel privacy harms, this direction also predictably produces suboptimal outcomes for businesses and consumers.

[11] *See, e.g.,* SAFE DATA Act (S. 4626, 116th).

The recent policy statement issued by the FTC interpreting its Health Breach Notification Rule is emblematic of the limitations and issues that can arise when the Commission stretches its limited powers beyond their intended purpose. During its most recent open meeting, FTC Commissioners voted 3-2 to approve a policy statement affirming that health apps and connected devices that collect or use consumers' health information must comply with the Health Breach Notification Rule. The FTC originally implemented its Health Breach Notification Rule in September 2009, as required as part of the American Recovery and Reinvestment Act of 2009, though it has yet to enforce the rule in its more than 10 years of existence. The rule requires that vendors of personal health records (PHRs) and their service providers notify consumers and the FTC when a breach of identifiable health information occurs. Failure to report such breaches carries civil penalties of up to $43,792 per violation per day.

With its new policy statement, the Commission goes to great lengths to elide the difference between a beach of security and a privacy violation in hopes of expanding the rule's reach. Whereas the Health Breach Notification Rule plainly states that it exists simply to ensure that PHR providers and their service providers notify consumers "when the *security* [emphasis added] of their individually identifiable health information has been breached,"[12] the policy statement asserts that whenever a health app *discloses* sensitive health information without users' authorization, this is a "breach of security" under the rule.[13] Notably, the Final Rule included several examples to elucidate what exactly a data breach means, all of which reference instances where information is taken or stolen *without* the provider's knowledge.[14] While we are sympathetic to the goal of preventing the unauthorized sharing of users' sensitive information and agree that there should be punishment when a company violates consumer trust, the fact remains a data breach notification law is an odd vessel to accomplish those goals.

The policy statement also stretches the definition of PHR, which is defined in the rule to mean "identifiable health information on an individual that can be drawn from *multiple sources* [emphasis added] and that is managed, shared, and controlled by or primarily for the individual." The policy statement instead asserts that health apps are covered by the rule even when the health information they collect comes from a single source (such as an application programming interface) and the user themself inputs non-health data, such as through a separate calendar app. This directly contradicts existing FTC business guidance on the very topic, which states that "[i]f consumers can simply input their own information on your site in a way that doesn't interact with personal health records offered by a vendor – for example, if your site just allows consumers to input their weight each week to track their fitness goals – you're not a PHR-related entity."[15]

The Health Breach Notification Rule is simply a poor fit for policing first-party privacy violations, and the FTC's new interpretation could create numerous unintended consequences along the way. For example, since the notification standard in the rule is triggered when the entity discovers the breach, FTC's interpretation seemingly blesses the underlying unauthorized sharing of data so long as the

---

[12] Health Breach Notification Rule, 74 Fed. Reg. 42962 (Aug. 25, 2009), *available at* https://www.ftc.gov/system/files/documents/federal_register_notices/2009/08/healthbreachnotificationrulefinal.pdf

[13] Federal Trade Commission, Statement of the Commission On Breaches by Health Apps and Other Connected Devices (September 15, 2021), *available at* https://www.ftc.gov/system/files/documents/public_statements/1596364/statement_of_the_commission_on_breaches_by_health_apps_and_other_connected_devices.pdf

[14] Health Breach Notification Rule, 74 Fed. Reg. 42966, §318.2 (August 25, 2009), *available at* https://www.ftc.gov/system/files/documents/federal_register_notices/2009/08/healthbreachnotificationrulefinal.pdf

[15] FTC Business Guidance, Complying with the FTC's Health Breach Notification Rule, *available at* https://www.ftc.gov/tipsadvice/business-center/guidance/complying-ftcs-health-breach-notification-rule

provider proffers a notification after the fact. Or, instead, should the provider notify consumers when it first discovers its own plan to share the information with third parties? That either answer to the policy statement's unanswered question generates a non-sensical outcome speaks to the frailty of the Commission's interpretation.

To be fair, the Commission is genuinely seeking to address a rather worrisome gap in our nation's current privacy framework. And as Commissioner Rebecca Kelly Slaughter indicated, she looks forward to the Commission "taking more action to limit the unfair collection and use of data, especially through rulemaking."[16] Commissioners want to make the most of the authorities they have and we appreciate that they are focused on healthcare privacy in particular. The productive use of healthcare data no longer only occurs with healthcare providers and other entities under the jurisdiction of the Health Insurance Portability and Accountability Act (HIPAA). The creation and flow of healthcare data outside the HIPAA umbrella has accelerated, even more so during the COVID-19 pandemic, and although the FTC has been active in enforcing its Section 5 authority, it does not possess first time enforcement authority to punish particularly egregious offenders.

These limitations were painfully illustrated in the recent settlement with Flo, a popular fertility and period tracking app that the FTC alleged shared the "health information of users with outside data analytics providers after promising that such information would be kept private."[17] Moreover, not only did Flo mislead consumers about its data sharing practices, but it also allowed third parties to use the data it shared for their own purposes.[18] In some cases, this occurred in violation of the terms of service of those third parties, the data having been shared via software development kits (SDKs) they provided to Flo.[19] These privacy missteps are especially concerning given the highly personal nature of the health information at issue.

Although Flo's core deceptive statements in this case enabled the FTC to enjoin further harmful conduct, existing statute limited the Commission's authority to wield monetary penalties to punish the company and signal to the marketplace that similar violations would not be tolerated. This is especially troublesome given that each and every headline detailing the deceptive conduct of firms using healthcare data outside the HIPAA umbrella threatens to further erode consumer trust, a key ingredient for success for our small business member companies. The healthcare innovations our member companies produce—from heart condition detection to chronic condition monitoring to simply managing digital health information across health systems—are far too important for us to let them fall victim to foundering consumer trust in digital health earned by bad actors.

---

[16] Statement of Comm'r Rebecca Kelly Slaughter Regarding the Comm'n's Policy Statement on Privacy Breaches by Connected Health Apps, Fed. Trade Comm'n, (Sept. 15, 2021), *available at* https://www.ftc.gov/system/files/documents/public_statements/1596320/rks_remarks_on_health_breach_policy_statement_09152021.pdf.

[17] Press release, "Developer of Popular Women's Fertility-Tracking App Settles FTC Allegations that It Misled Consumers About the Disclosure of their Health Data," Fed. Trade Comm'n (Jan. 13, 2021), *available at* https://www.ftc.gov/news-events/press-releases/2021/01/developer-popular-womens-fertility-tracking-app-settles-ftc.

[18] Fed. Trade Comm'n, Flo Health, Inc., complaint (published Jan. 13, 2021), *available at* https://www.ftc.gov/system/files/documents/cases/flo_health_complaint.pdf.

[19] *Id.*

From our perspective, the answer is not for the FTC to create novel or tenuous interpretations of its existing rules nor is it to extend HIPAA to cover healthcare tools and services not currently subject to HIPAA. As we've shown, the Commission will inevitably encounter roadblocks as it seeks to retrofit old rules to address new use cases. Meanwhile, HIPAA's overarching purpose is to ensure the portability of health data between covered entities and business associates, and it was not primarily designed to give consumers better control over their own healthcare data or to manage the risks healthcare data processing poses.

III. Congress Should Enact a Federal Privacy Framework

In our opinion, the best way to improve FTC enforcement capabilities within the privacy sphere is to specifically grant those authorities as part of a federal privacy framework.
We urge the Committee to establish a set of federal requirements that puts in place baseline consumer rights and curbs data processing activities that expose consumers to undue privacy risks. For example, legislation introduced by the Committee chair and ranking member, as well as bipartisan draft legislation circulated by House Energy and Commerce Committee staff last year were a positive start representing substantial agreement on aspects of privacy that previously struggled for consensus. We urge you to continue the work on this effort and we stand ready to support negotiations and oversight activities around it.

Specifically, the App Association supports a federal framework with the following attributes:

- **Transparency**
  - Federal privacy requirements should ensure businesses are transparent about the collection and use of information about consumers. App Association members compete on privacy and work hard every day to develop better ways to communicate with their users about privacy and give them meaningful choices. Consumers should have a clear understanding of the types of personal data they are sharing, and which companies are using that data and how.
- **Strong consumer rights**
  - A federal law should empower consumers to exert more control over their personal information, including the rights to access, correction, and deletion of such information. Sensitive personal information should also be subject to some limits on processing activities that pose too great a risk to consumers, which is not outweighed by countervailing benefits.
- **Accountability**
  - As the FTC has long argued, privacy should be built into the design and functionality of products and services. If privacy is a functional feature of a product or service, the protections, notices, and options it provides may shift and take on different forms depending on the context. Federal law should support the dynamic functionality of privacy by design by making companies accountable for sound privacy practices while allowing them to innovate on the details of their privacy programs.
- **A single, national standard**
  - New privacy legislation in Congress should establish a single, national standard and avoid creating a patent troll-style business model for trial attorneys to sue and settle with small companies through a broad private right of action. Our member companies may include the smallest software and connected device companies, but they each serve consumers across the nation and around the world. Complying with a patchwork

of state laws would be unnecessarily burdensome because their activities are not limited by any single state's borders. If privacy legislation does include a preemption provision, we would support limited rulemaking authority within statutory guidelines and limits for the FTC and allowing state attorneys general to enforce the bill's provisions.

- **Scalable requirements**
  - Federal privacy requirements should be scalable depending on the scope of an enterprise or data processing activities and the size and compliance capabilities of companies. App Association members do not want to be exempt from requirements—they want to comply with strong, flexible, and reasonable requirements.

Additionally, though several promising frameworks passed into law this year at the state level, including in Virginia and Colorado, we do not recommend that Congress wait around until the states cobble together a privacy patchwork that covers the nation. Despite recent progress, at the current pace of passage, it would take decades for the individuals of all 50 states to gain coverage. Needless to say, Congress should not stand by idly as data abuses continue to proliferate in the states that opt against or are unable to pass a law.

Moreover, the more states that pass laws the greater the ambiguities and contradictions for businesses and consumers. Each of the three state privacy laws currently on the books include varying definitions for key terms, applicability thresholds, and sectoral exemptions. As more states enter the fray with their own laws, those nuances are only likely to multiply which makes compliance exponentially more difficult for businesses that operate across state lines (or have consumers in multiple states), while also increasing consumer confusion as to how their rights may or may not apply in a given scenario.

Finally, each new state law also improves the odds of a dormant Commerce Clause challenge, especially insofar as a new law directly contradicts another state privacy law or takes aim at a specific industry.[20] While this issue has yet to rear its head given the low number of state privacy proposals to make it from bill to law thus far, a constitutional challenge under the Commerce Clause could quickly stall the moderate progress at the state level bringing us back to square one. A preemptive federal law is the only option that can avoid legal uncertainty, while effectuating uniform consumer rights across the nation at the same time.

IV. Congress Should Avoid Antitrust Measures that Presume the Illegality of Platform-Level Privacy Protections

Software platforms (app stores together with mobile operating systems) play a key role in managing an app ecosystem that offers consumers a wide variety of options, while minimizing privacy risks. These management functions form the core of the bundle of developer services App Association members purchase from platforms, without which consumer trust would be undermined. Some proposals in Congress, like the American Choice and Innovation Online Act (H.R. 3816) would

[20] Jennifer Huddleston and Ian Adams, "Potential Constitutional Conflicts in State and Local Data Privacy Regulations", Regulatory Transparency Project of the Federalist Society, (December 2, 2019), *available at* https://regproject.org/wp-content/uploads/RTP-Cyber-and-Privacy-Paper-Constitutional-Conflicts-in-Data-Privacy-final.pdf

presumptively prohibit these management functions, ostensibly to address complaints from competitors with alternative products and services on the platform. H.R. 3816 does this by prohibiting a software platform from conduct that "excludes or disadvantages the products, services, or lines of business of another business user . . . relative to the [platform's] own"[21] offerings. While the bill would benefit some large competitors like Epic Games and Spotify, it would harm small app makers like App Association members as well as consumers because they would erode the trust consumers have in conducting digital commerce in the app marketplaces.

H.R. 3816's prohibitions create a presumption that many platform-level privacy controls are illegal, which platforms could overcome only in especially narrow circumstances. The bill would essentially allow platforms to overcome that presumption only by showing that any measure they take was "narrowly tailored, could not be achieved through a less discriminatory means, was nonpretextual, and was necessary"[22] to provide privacy. This construct is in tension with the FTC's focus on privacy by design and its privacy enforcement against bad actors on the app stores. It is also inconsistent with App Association members' calls for platforms to expeditiously remove harmful and fraudulent content.[23] In fact, a recent FTC settlement illustrates how a statutory mandate for app stores to allow unvetted software onto smart device operating systems could harm consumers' privacy and security. On September 1, 2021, the FTC published an initial complaint, along with a unanimously approved settlement, with SpyFone.[24] According to the complaint, SpyFone marketed itself as a surveillance app, enabling purchasers to track targets in a variety of ways, including by spying on live location, web history, contacts, pictures, calendar, files downloaded onto a device, notifications, emails, video chats, and even social media posts.[25] The company explained to its users how to download the app on a target's device, hide the app so the target would not notice its presence, and bypass Android operating system controls in order to track the target without their knowledge.

Stalkerware apps could easily claim that iOS and Android have similar offerings because their legitimate uses, as marketed, involve parents managing their children's devices. In this scenario, Android clearly disadvantages SpyFone versus its own offerings by forcing it to go through onerous steps in order for a purchaser to make use of the app. For example, Android forces SpyFone to have its purchasers enable the sideloading capability, which triggers a warning from Android that "[i]f you download apps from unknown sources, your device and personal information can be at risk. Your device could get damaged or lose data. Your personal information could be harmed or hacked."[26] Certainly, these additional steps and a warning like this hurt SpyFone's business. Likewise, iOS disadvantages SpyFone versus its own offerings because it does not allow SpyFone on iOS devices at all. And the affirmative defense H.R. 3816 provides in cases where a software platform needs to remove an app for violating a law or threatening consumer privacy does nothing to help because as drafted it is so inaccessible as to discourage any sort of reliance on it. The overall effect of H.R. 3816 in the stalkerware context is to create a default rule barring the removal of stalkerware like SpyFone from a platform, as well as any privacy-related barriers that prevent stalkerware from taking

[21] American Choice and Innovation Online Act (H.R. 3816, 117th).
[22] American Choice and Innovation Online Act, Sec. 2(c)(1)(B) (H.R. 3816, 117th).
[23] Statement of Morgan Reed, president, ACT | The App Association, on App Store Review Fraud Scheme (Feb. 11, 2021), *available at* https://actonline.org/statements/.
[24] Press release, Fed. Trade Comm'n, "FTC Bans SpyFone and CEO from Surveillance Business and Orders Company to Delete All Secretly Stolen Data" (Sept. 1, 2021), *available at* https://www.ftc.gov/news-events/press-releases/2021/09/ftc-bans-spyfone-and-ceo-from-surveillance-business.
[25] Fed. Trade Comm'n, Complaint, *In the Matter of Support King, LLC, and Scott Zuckerman*, 192 30003 (Sept. 1, 2021), *available at* https://www.ftc.gov/system/files/documents/cases/192_3003_spyfone_complaint.pdf (SpyFone Complaint).
[26] SpyFone Complaint at para. 6.

advantage of consumers, unless a platform is able to overcome that presumption, likely in narrower forms, on a case-by-case basis.

The bottom line is that taking a nondiscrimination sledgehammer to software platforms' role in removing bad actors rolls out the red carpet for apps like SpyFone. More importantly, by widening the avenues for fraudsters on app stores, an overbroad federal nondiscrimination regime would narrow the path for smaller app makers like App Association members. It would also make the FTC's job in enforcing the statutory prohibition on unfair or deceptive acts or practices that much more difficult, as more bad actors enter the fray and less of their activity is discoverable because platforms' hands would be tied. Meanwhile, as consumers adjust to a more fraud and malware-ridden marketplace, they would rationally shift away from experimentally downloading apps with the shortest histories and smallest preexisting distribution in favor of bigger brands. What is now a high trust environment, thanks in no small part to rigorous gating, would then evolve into a no-trust environment, which disproportionately harms smaller companies while benefiting the platform's largest "business users." The effect would be similar with measures like the Open App Markets Act (S. 2710), which takes a narrower approach but still creates a presumption that platform gating functions to protect privacy are illegal.

We urge the Committee to avoid measures like these in their current form, because they would move federal privacy policy in the opposite direction from where it should be heading. Congress should not *prohibit* (or presume the illegality of) privacy controls that are proven to work; instead, it should *require* companies to adopt privacy protections. Otherwise, federal law would undo the privacy-protective developments that enable online commerce, forcing consumers to accept a single, more open approach to security, or even worse, bring us back to an early 2000s online experience with fewer options, less meaningful privacy protections, and diminished security.

V. Conclusion

We appreciate that the Committee seeks our views on approaches to bolstering the FTC’s ability to address consumer privacy more effectively in the wide variety of industries it oversees and in which App Association members compete. Federal privacy law is overdue for an update to meet the challenges of the 21st century. App Association member companies want stronger federal privacy requirements in particular, including a single set of national rules governing authorized data processing activities and data security practices. This Committee has made unprecedented bipartisan progress toward agreement on a national privacy law, and we urge that this hearing and further Committee activities help inform that process.

Appendix: App Economy Innovators in Your Districts

Majority

Chair Maria Cantwell (WA)
Company: Mighty Call

Located in Spokane, Mighty Call is a cloud-based communications and customer service platform founded in 1999. Their virtual phone system is designed specifically for small businesses and remote teams making it easy for teams to connect from anywhere through mobile and desktop apps. Their apps provide unique features like call availability windows, scheduling services, and the ability to mask personal cell numbers, given that privacy is a core pillar of Mighty Call's service.

Senator Amy Klobuchar (MN)
Company: Vēmos

Located in the Twin Cities and founded in 2013, Vēmos is a platform solution for bars, restaurants, and other venues as a one-stop-shop for the digital tools needed to manage and grow their businesses. Operating with only eight full-time employees, Vēmos found a way to harness and present a venue's data in a humanized way, which helps venues understand who their customers are and how to market to them effectively.

Senator Richard Blumenthal (CT)
Company: Pixellet

Located in Stamford, Connecticut, Pixellet is a full-service web and mobile development and design firm with dozens of offered services, including digital marketing and ecommerce. Founded in 2014, Pixellet only has one employee and has served a variety of industries including real estate, health care, financial services, and education, among others.

Senator Brian Schatz (HI)
Company: Smart Yields

Founded in 2015 and headquartered in Honolulu, Smart Yields is an intelligent agriculture software that helps to connect farmers and agricultural researchers to increase crop yield, revenue, and productivity. With fewer than 10 employees, Smart Yields is committed to helping Hawaii meet their commitment to doubling food production by 2030 and other communities achieve similar goals around the world.

Senator Ed Markey (MA)
Company: Podimetrics

Established at the Massachusetts Institute of Technology in 2011, Podimetrics is a medical technology services company that develops hardware-enabled, thermal-imaging solutions to predict and prevent diabetic foot ulcers. The Podimetrics SmartMat™ monitors the temperature of diabetes patients' feet to identify temperature asymmetries that signal the development of a foot ulcer. Coupled with a monitoring service, the Podimetrics Remote Temperature Monitoring System™ uses the wireless SmartMat™ to notify patients and clinicians of temperature asymmetry and inflammation, the first signs of foot ulcers preventing amputations and other health complications.

Senator Gary Peters (MI)
Company: Workit Health
Workit Health is a women-owned digital therapeutics company based in Ann Arbor that is focused on treating addiction. Their Workit Health app connects patients with clinicians and a community, allowing individuals to receive the communal support necessary for addiction treatment, and routine contact with mental health and clinical care givers in the discreet privacy and safety of their home or preferred treatment site.

Senator Tammy Baldwin (WI)
Company: Birdwell Solutions
Founded in Madison in 2019, Birdwell Solutions is a concierge software development agency focused on working with entrepreneurs and startups to build web, digital, and mobile products that help their clients launch and grow their business. With a team that ranges from full stack development to design and project management, Birdwell Solutions is working to foster and support the entrepreneurial community in Wisconsin.

Senator Tammy Duckworth (IL)
Company: Devscale
Founded in 2018, Devscale is a custom app development company with a focus on product strategy. With clients that range anywhere from small to large, Devscale helps their clients through problems in their digital strategy with a trained eye on unique user experiences and a transparent development cycle. Although headquartered in Chicago, Devscale has coders all over the world. They take clients all the way through their creative process; from defining the project through user experience stages and development, to the final rollout.

Senator Jon Tester (MT)
Company: Guidefitter
Headquartered in Bozeman, Guidefitter is an online and mobile platform that connects people with guides, nature experts, and sportspersons for safe and guided natural expeditions and sport including hunting, fishing, hiking, and camping. The platform also allows the experts to promote their business or experience and facilitates payment for merchandise as well as the guided tour or event.

Senator Kyrsten Sinema (AZ)
Company: Devsoft Group
Devsoft Group is a one-man custom development firm founded in 2010. Focused on clients in manufacturing and energy, Devsoft Group works closely with their clients, building web, cloud, SaaS, and mobile and database solutions that meet the unique needs of each client's projects and business needs.

Senator Jacky Rosen (NV)
Company: Pigeonly
Pigeonly is an online and mobile platform that connects inmates with their loved ones. Their services provide a central place to send letters, pictures, cards, and more. Through the platform, families can also call their inmate at a lower cost and stay in touch throughout their incarceration. The company's mission is to improve communication and community for those incarcerated and to encourage families to stay in touch with their inmates by simplifying and streamlining the process.

Senator Ben Ray Luján (NM)
Company: Snowball
Snowball is an all-in-one fundraising platform that connects users with more than 15,000 nonprofits across the country. The app has two parts. The first is for donors, giving them information about the nonprofits in Snowball's network, donation opportunities, and notice of emergency relief needs, and provides a secure place to track donations and save credit card information. The second, for nonprofits, helps to keep track of donors, grow their donor base, and communicate opportunities.

Senator John Hickenlooper (CO)
Company: Atelier
Atelier is a mobile app that allows users to create their own interior design, discover planet-conscious makers of furniture, textiles, art, and more. Through the app, users can design a room and then create 3D images of their designs giving them a clear sense of the finished process. The app also allows users to purchase the pieces they used in their design, supporting small and eco-conscious creators.

Senator Raphael Warnock (GA)
Company: Rimidi
Rimidi creates mobile apps that work directly within electronic health records (EHR) to combine patient-generated health data with clinical data, allowing for patient-specific clinical insights. They have developed a COVID-19 screening application based on the widely accepted Fast Healthcare Interoperability Resources (FHIR) standard for health systems to identify and flag at-risk patients via survey prior to existing appointments. Their tool enables health systems to mitigate the spread of COVID-19, as well as optimize treatment.

Minority
Ranking Member Roger Wicker (MS)
Company: Buzzbassador
Buzzbassador is a management platform for brands that uses ambassadors to promote their products across social media. The platform gives brands the tools to track social media posts, engagement metrics, sales, commission payouts, and more for each of their ambassadors and provides simple analytic reports and a central dashboard.

Senator John Thune (SD)
Company: Infotech Solutions, LLC
Infotech Solutions, LLC is a concierge IT service helping businesses with everything from implementing a new software system or network to maintenance, general IT issues, security, and more. The company also offers an app across platforms that helps their clients troubleshoot IT issues, connect with their IT service team, and more.

Senator Roy Blunt (MO)
Company: Topik
In 2015, two friends co-founded Topik, a mobile blogging application that makes it easy for anybody to create and share blog posts on an easy-to-use mobile platform. Based in St. Louis, Missouri, Topik is completely self-funded and, with only two employees, is set to launch their first mobile app later this year.

Senator Ted Cruz (TX)
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 individualized supports and accommodations that meet ADA requirements.

Senator Deb Fischer (NE)
Company: Quantified Ag
Quantified Ag is a tracking device and platform to monitor cattle health and enables farmers to quickly remove sick or injured cattle from the rest of the herd to treat them quickly and prevent further infection. The device, worn on the cow's ear, monitors the cow 24/7 and connects seamlessly with the Quantified Ag mobile app allowing ranchers and farmers to easily monitor their cattle throughout the day. Recently acquired by Merck, Quantified Ag built and continues to run the business from Nebraska.

Senator Jerry Moran (KS)
Company: ActiveLogic Labs
ActiveLogic Labs is an innovative digital development agency headquartered in Kansas City with a growing presence across the United States, including an office in the Chicago area. They provide a number of services from web and desktop software development to mobile app development, all with a specific focus on user interface design and a seamless user experience.

Senator Dan Sullivan (AK)
Company: StepAway
StepAway is a mobile application to help those with addiction manage their day-to-day and make better decisions about their daily habits to help prevent relapses. The app is primarily centered around those who are unable to seek addiction treatment services but are looking to make a change in their drinking habits. The app helps track daily progress while also giving users insight in their triggers, and provides useful information on how to make different and better decisions related to their alcohol use in a safe and private space.

Senator Marsha Blackburn (TN)
Company: Quiet Spark
Established in 2011 in LaVergne, Tennessee, a wife and husband team founded Quiet Spark after noticing their son's issues with spelling. Their first app was SuperSpeller, an iOS app that makes learning spelling fun for children through learning games and reward features. They have also created other apps that help users keep track of their lives through categories like exercise, reading time, scheduling, homework, and more.

Senator Todd Young (IN)
Company: InGen Technologies, Inc.
InGen Technologies, Inc., is a software consultancy company focused on improving customer experience for their clients and improving data collection and analysis tools to improve their clients' use and understanding of data analytics. The company's mission is to unite all aspects of their clients' digital presence from apps to the web in order to improve overall digital marketing and cohesiveness.

Senator Mike Lee (UT)
Company: 1564B
Located in Salt Lake City, 1564B is a one-man management consulting group that provides advice on marketing and content development as it relates to technical markets, like the internet of things (IoT). Founded in 2014, 1564B's clients range from startups and growing companies to global corporations.

Senator Ron Johnson (WI)
Company: Xorbix Technologies
Founded over 20 years ago with a location in Hartland, Xorbix Technologies is a custom software development firm helping businesses meet their customers online. They offer a number of services such as full-service custom software development, mobile app development, and general IT consulting.

Senator Shelley Moore Capito (WV)
Company: TMC Technologies
TMC Technologies is an IT services company focused on helping their clients, both federal and local, with program and project management, scalable system and software engineering, IT infrastructure design and management, and network and telecom services. TMC Technologies has focused a lot of their IT work in their own backyard providing IT services for West Virginia companies, especially small business owners, looking to bring their company into the digital age.

Senator Rick Scott (FL)
Company: Thinkamingo
Founded in 2011, Thinkamingo is an educational app company focused on getting kids excited about writing. Their app, Story Dice, helps give kids ideas for stories, while their apps Lists for Writers and Story Spark help kids lay out their story, build out their characters and plot points, and give them the tools they need to improve their overall writing and story structure.

Senator Cynthia Lummis (WY)
Company: BlackFog
BlackFog is a cyberthreat prevention company that uses a unique combination of behavioral analysis and data exfiltration technology to identify, stop, and prevent future data hacks, unauthorized data collection, and more across mobile and web endpoints. Their services protect their clients and their clients' most sensitive data and privacy while also strengthening their regulatory compliance.