July 29, 2024

The Honorable Cathy McMorris Rodgers
Chair
House Committee on Energy
and Commerce
Washington, District of Columbia 20515

The Honorable Frank Pallone
Ranking Member
House Committee on Energy
and Commerce
Washington, District of Columbia 20515

The Honorable Gus M. Bilirakis
Chairman
House Committee on Energy
and Commerce
Subcommittee on Innovation, Data,
and Commerce
Washington, District of Columbia 20515

The Honorable Janice D. Schakowsky
Ranking Member
House Committee on Energy
and Commerce
Subcommittee on Innovation, Data,
and Commerce
Washington, District of Columbia 20515

Re: The FTC needs to adopt a balanced regulatory approach that prioritizes consumer welfare.

Dear Chair Rodgers, Ranking Member Pallone, Chairman Bilirakis, and Ranking Member Schakowsky:

ACT | The App Association writes to convey our appreciation for your recent oversight efforts and to emphasize the importance of the FTC remaining focused on consumer welfare and adhering to its statutorily-bound duties. The App Association is the leading trade group representing small businesses in the app economy. Today, The App Association represents an ecosystem valued at approximately $1.8 trillion and is responsible for 6.1 million American jobs.[1] Our members are innovators that create the software bringing your smart devices to life. They also make all the connected devices that are revolutionizing healthcare, agriculture, public safety, financial services, and virtually all other industries. They propel the data-evolution of these industries and compete with each other and larger firms in a variety of ways, including on privacy and security protections.

Consumer trust is fundamental for competitors in the app economy, especially for smaller firms that may not have substantial name recognition. We appreciate the Subcommittee's emphasis on safeguarding consumer welfare while considering the regulatory burdens on businesses. The Federal Trade Commission (FTC) plays an important role in this mission but needs to be more accountable to Congress and stay within its statutorily-bound duties. The FTC must be careful not to adopt broad rulemaking that would invite serious security, privacy, and intellectual property (IP) risks

[1] ACT | The App Association, *State of the U.S. App Economy: 2023*, https://actonline.org/wp-content/uploads/APP-Economy-Report-FINAL-1.pdf

for U.S. businesses. In particular, the FTC should focus on protecting consumers from real harm rather than theoretical objectives and hypothetical threats. We write to urge the Subcommittee to consider the following recommendations for the FTC to protect[2] consumer welfare while not stifling small business innovation.

FTC Rulemaking on Privacy Harms Innovation and Oversteps Authority

The FTC's Advance Notice of Proposed Rulemaking (ANPR) on "Commercial Surveillance and Data Security" proposes a path that would far exceed the FTC's own authority. Subtly adopting the marketing term "commercial surveillance" advertises the conclusion the FTC has likely already drawn in this inquiry: that using data to provide products and services is inherently harmful and only the FTC can save consumers from letting companies do so on their behalf. Any serious policymaking effort on privacy cannot begin with such a poisoned premise and instead must focus on empowering consumers and innovators to leverage data in privacy-protective ways. Now more than ever, small businesses and startup innovators rely on a competitive, trustworthy, and secure ecosystem to reach millions of potential users across consumer and enterprise opportunities so they can grow their businesses and create new jobs. Since 1915, the FTC has applied its authority and developed expertise to address new technologies and market scenarios, often relying on its authority to adjudicate issues arising under Section 5 of the FTC Act on a case-by-case basis.[3] While the Commission is authorized to propose "rules which define with specificity acts or practices which are unfair or deceptive acts or practices [UDAP] in or affecting commerce"[4] within the meaning of Section 5(a)(1) of the Act, it is far from certain that the FTC has the authority to wield broad rulemaking power.[5] Further, the legislative history does not add a penumbra of authority around the ability to define specific UDAP sufficient to authorize the kind of fishing expedition it has embarked upon with the ANPR.

Privacy remains a critical issue in policymaking within the digital age. The current American privacy framework is evolving, and the App Association recognizes the urgent need for reform in how privacy is regulated in the United States. The blend of federal regulations specific to certain sectors and a variety of state laws create a complex landscape that is particularly challenging for innovative small businesses. For the following reasons, privacy policymaking must belong within the purview of the legislature and not the FTC.

FTC Lacks Authority to Promulgate a National Privacy Standard. The Supreme Court in *West Virginia v. EPA* affirmed the Major Questions Doctrine and the legal principle that in cases of vast economic and political significance federal agencies must

[2] *See* Transforming the FTC: Legislation to Modernize Consumer Protection, hearing before the House Committee on Energy and Commerce, Subcommittee on Consumer Protection and Commerce, 117th Cong. 1st Sess., testimony of Graham Dufault, Senior Director for Public Policy, ACT | The App Association (Jun. 14, 2021), *available at* https://actonline.org/wp-content/uploads/2021-07-27-ACT-CPC-Subcommittee-Testimony-FINAL1.pdf.
[3] Federal Trade Commission Act § 5, 38 Stat. at 719-21; and 15 U.S.C. § 45 (2018).
[4] 15 U.S.C. Sec. 57a (2028).
[5] 87 FR 51273; Federal Trade Commission Act Pub. L. No. 63-203, § 6(g), 38 Stat. 717, 722 (1914).

have clear authorization from Congress to make rules. As noted, data is critical to the basic business decisions of all American companies, and it is clear a national privacy and security rule would have major economic and political consequences. California's first set of privacy regulations alone was estimated to cost companies a total of $55 billion in compliance costs.[6] A national privacy rule would have a much larger effect. A comprehensive privacy and security regulation would likely run afoul of the Major Questions Doctrine because Congress has not specifically authorized a nationwide data protection law.

A Privacy Rule Would Further a Burdensome National Privacy Patchwork. A comprehensive privacy, security, and algorithmic rule would complicate the existing patchwork of state privacy laws. Because the FTC's authorities under Section 5 likely would not be preemptive, a new national rule would add a new layer of regulation that would further confuse consumers and make compliance even more difficult for companies, particularly small businesses. A new national layer of regulation to a state patchwork would disproportionately impact small businesses as they would not have the same resources for compliance as larger firms. According to a report by the Information Technology and Innovation Foundation (ITIF), a 50-state patchwork of laws could cost the economy one trillion dollars over 10 years, with small businesses alone taking a $200 billion hit.[7]

The App Association is committed to a strong FTC acting to address demonstrated consumer harms and has continuously supported FTC enforcement actions to protect consumers. The App Association is supportive of a new federal privacy framework that will clarify the obligations of our members and preempts the fractured state-by-state privacy compliance environment, and generally urges that the U.S. approach to privacy provide robust privacy protections that correspond to Americans' expectations, as well as leverage competition and innovation.[8] We have urged the FTC to carefully consider whether its recent advance notice of proposed rulemaking, while well-intentioned, could derail increasingly promising efforts by Congress to advance a new cross-sectoral privacy framework.[9] The App Association has recommended that the FTC instead consider providing guidance, which it has the ability under its existing authority to, on consumer privacy while Congress' work on new legislation continues.

---

[6] Lauren Feiner, *California's new privacy law could cost companies a total of $55 billion to get in compliance*, CNBC (Oct. 5, 2019), https://www.cnbc.com/2019/10/05/california-consumer-privacy-act-ccpa-could-cost-companies-55-billion.html.
[7] ITIF Information Technology & Innovation Foundation*, 50-State Patchwork of Privacy Laws Could Cost $1 Trillion More Than a Single Federal Law, New ITIF Report Finds*, ITIF (Jan. 24, 2022), https://itif.org/publications/2022/01/24/50-state-patchwork-privacy-laws-could-cost-1-trillion-more-single-federal/.
[8] Morgan Reed, *Big questions for small businesses in the American Privacy Rights Act*, IAPP (June 7, 2024), https://iapp.org/news/a/big-questions-for-small-businesses-in-the-american-privacy-rights-act.
[9] Graham Dufault, *The 4 Ps of Privacy: What Small Businesses Need in a Privacy Bill*, ACT | The App Association (Sept. 13, 2022), https://actonline.org/2022/09/13/the-4-ps-of-privacy-what-small-businesses-need-in-a-privacy-bill/.

In today's market, privacy protection is a key differentiator. We have cautioned the FTC against disrupting this dynamic within the digital economy. Additionally, we have urged the FTC to base its policy actions on solid, data-driven evidence and not on rare or hypothetical scenarios.

Beyond HBN Rule Expansion: There is a Critical Need for Federal Legislative Authority in Health Data Privacy

The FTC originally implemented its Health Breach Notification (HBN) Rule in September 2009, which the American Recovery and Reinvestment Act of 2009 required. This 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.

The App Association shares the FTC's commitment to advancing responsible health data stewardship and privacy throughout the continuum of care and recognizes that no data is more personal to Americans than their health data. The App Association's members acknowledge that significant threats to Americans' most sensitive data continue to evolve and put extensive resources into ensuring the security and privacy of health data to earn the trust of consumers, hospital systems, and providers. Breach notification requirements generally serve important functions. They not only notify the individual when their information has been compromised, but they also provide insight into security issues that organizations may be facing.

However, digital health innovators do struggle to navigate the complex environment with respect to cybersecurity and privacy as they contend with Health Insurance Portability and Accountability Act (HIPAA) requirements at times and relevant FTC requirements at others, on top of state-specific requirements that can vary significantly. Further, the first enforcement case under the HBN Rule only occurred in 2023. We are concerned that the FTC's expansion of its HBN Rule[10] could be interpreted by some, including Congress, as reducing the need for this long overdue legislation. From our perspective, however, the answer to the health data protection gap is not for the FTC to create novel interpretations of its existing rules nor is it to extend HIPAA to cover healthcare tools and services not currently subject to HIPAA.

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. To this end, the App Association supports the development of a new cross-sectoral privacy framework by Congress in the form of a general federal privacy framework. As part of such a solution, we support the proposition that any such general privacy bill treats health data as a subclass of "sensitive" personal information subject to heightened regulatory requirements, including with respect to breach notification requirements.

[10] 89 CFR 47028.

The additional authority that such a legislative framework will provide the FTC will be critical in advancing consumer and patient privacy and trust. Until that time, innovators in the digital healthcare ecosystem have to continue to dedicate valuable resources to tracking and complying with the range of state data breach laws and regulations, some of which conflict or overlap with FTC HBN rules.

The FTC's Proposed Negative Option Rule Curtails Market-Driven Solutions in the Tech Sector

The FTC has also proposed updates to its rules around certain kinds of subscription arrangements, where subscribers have the option to "opt out" of a subscription agreement rather than being asked to specifically "opt in." Any updates to the Negative Option Rule must include significant flexibility for companies to design subscription services for their customers. By continuing to have an adaptable regulatory regime for more subscription plans, it will encourage new innovative approaches in consumer transparency. The small tech community appreciates the FTC's efforts to clarify the regulatory landscape to benefit consumers. However, the FTC's recent proposed rule[11] does not simply condense requirements into one rule but includes an improperly expanded scope that would adversely impact the growth of the small technology community that utilizes continuity plans, automatic renewals, and free (or partially free) trials that convert to paid subscriptions, without any public benefit. In comments before the FTC, the App Association asked it to withdraw its proposed rule and undertake meaningful and inclusive outreach to our diverse community of small business developers, along with other impacted stakeholders, to inform its next steps and whether the FTC's existing authority provides it with the tools it needs to address demonstrated harms stemming from negative option practices.

Building trust through transparency with consumers is a top priority for the small technology businesses we represent. However, the proposed rule presents an additional regulatory barrier to effectively running their business. As regulators from across key markets abroad continue to utilize regulatory approaches for the digital economy which are often heavy-handed, the United States has remained the greatest market in the world for building a startup due to its evidence-based and light-touch approach to regulating new industries. Across the world, other governments struggle to incent and sustain the digital economy growth seen only in this country because companies elsewhere often face greater barriers to bringing novel products and services to market—slowing technological innovations to the pace of government approval. Now more than ever, the small business and startup innovators we represent rely on a clear and consistent legal and regulatory landscape to foster a trustworthy and secure environment to reach millions of potential users across consumer and enterprise opportunities so they can continue to grow their businesses and create new jobs. Driven by U.S. small businesses, the hyper-competitive app economy continues to grow, offering immense opportunity to small business developers. Our members recognize that transparency and communication are crucial ingredients to success in this environment, and work to find new and innovative ways to meet consumer expectations.

[11] 88 FR 24716.

Should a small business fail to meet customer expectations with respect to transparency or communication, the market provides numerous alternatives for those customers, a well-recognized characteristic of a competitive marketplace.

The App Association has urged the FTC to recognize the highly competitive nature of the app economy and its benefits, and to further ensure that any regulatory changes made to the Negative Option Rule do not disrupt its pro-consumer benefits.

FTC's Focus Should be to Uphold Consumer Protection within Statutory Limits, Not Seek Outcomes Beyond its Mandate via Trade Talks

Recently, the FTC has significantly shifted from its foundational mission of safeguarding consumers and promoting fair competition. The agency now oversteps its regulatory authority, sidelines due process, and flouts traditional norms. This pivot raises concerns about undermining the established checks and balances within the U.S. governance structure.

Moreover, the FTC has intensified its cooperation with foreign regulators, notably supporting the European Union's (EU) stringent regulations on major U.S. technology companies. This international collaboration has encouraged the implementation of the EU's Digital Markets Act (DMA) and Digital Services Act (DSA), which impose disproportionate burdens on the American firms they regulate directly and the small companies that leverage online marketplaces. The DMA compels designated "gatekeeper" companies—primarily American—to share customer data with third parties under threat of hefty fines. Similarly, the DSA imposes rigorous audit and data sharing requirements on large online platforms, predominantly U.S.-based, again with significant financial penalties for non-compliance. While these measures claim to bolster consumer protection and competition, they strategically weaken U.S. corporations to benefit European and other non-U.S. competitors.

In addition, the FTC's engagement with U.S. Trade Representative (USTR) negotiations leading to USTR's sudden withdrawal from digital trade priorities at the World Trade Organization, apparently without consulting Congress or other federal agencies, points to a concerning pattern.[12] Such unilateral actions by the FTC, as part of a broader antitrust agenda, threaten not only the digital trade safeguards that smaller companies rely on but also the broader economic interests of the United States.

This international involvement undermines U.S. sovereignty and Congress' legislative authority, risking the global competitiveness of U.S. firms and potentially affecting the financial well-being of American investors, including those with retirement savings in these companies. Rather than assisting foreign governments and institutions in crafting policies that disadvantage American businesses, the FTC should refocus on tackling

---

[12] Graham Dufault, "The Effort to De-Democratize Tech Entrepreneurship Goes Global," ACT | THE APP ASSOCIATION BLOG, (Nov. 9, 2023), available at https://actonline.org/2023/11/09/the-effort-to-de-democratize-tech-entrepreneurship-goes-global/.

domestic issues such as market fraud and deception, using its well-established legal authority under the FTC Act, the Fair Credit Reporting Act, and the Equal Credit Opportunity Act. These laws empower the FTC to effectively address and penalize unfair or deceptive practices that harm consumers, thereby realigning with its core mission.

The FTC has also Recently Sought to Achieve Competition Goals That Would Harm Small Businesses in the App Economy and Consumers

Outside of this Subcommittee's jurisdiction, but of interest in the context of FTC budget discussions, the FTC has recently sought to prohibit business practices that benefit small app companies by reinterpreting its unfair methods of competition (UMC) authority. For example, it issued a new UMC enforcement policy with virtually no limits at all and a focus on prioritizing protections for well-resourced competitors;[13] brought a case against Amazon that could illegalize many offerings from curated online marketplaces that small businesses rely on;[14] and engaged in a campaign to end the ability for small businesses to be acquired,[15] to name just a few examples. The campaign to kill mergers and acquisitions is especially problematic for small companies in the app economy and is another instance where the FTC has gone to its European counterparts to achieve an end result that is not allowed under U.S. law (in this case because the merger itself was procompetitive).[16]

Conclusion

As the Subcommittee deliberates on the Fiscal Year 2025 Federal Trade Commission Budget, we strongly urge it to reevaluate the FTC's priorities. The App Association advocates for the FTC to focus on tangible consumer protection within its statutory boundaries, thereby avoiding regulatory overreach that could threaten the vitality of the U.S. tech sector and the broader economy. By prioritizing effective, data-driven enforcement within its established legal framework, the FTC can better support American businesses and consumers. It is crucial that the FTC avoid broad, undefined rulemaking that could suppress innovation and infringe on consumer rights. We value the Subcommittee's commitment to maintaining a healthy regulatory environment that supports, rather than hampers, the vital app ecosystem integral to our economy.

---

[13] Ted Bolema, "What Does the New Federal Trade Commission Policy Statement Mean for Antitrust?" THE CENTER FOR GROWTH AND OPPORTUNITY, (Sept. 5, 2023), *available at* https://www.thecgo.org/research/what-does-the-new-federal-trade-commission-policy-statement-mean-for-antitrust/.

[14] ACT | THE APP ASSOCIATION, ISSUE BRIEF: WHY APP DEVELOPERS CARE ABOUT FTC V. AMAZON (Oct. 5, 2023), *available at* https://actonline.org/2023/10/05/issue-brief-why-app-developers-care-about-ftc-v-amazon/.

[15] Graham Dufault, "Killing Commerce for Dummies: A How-To Manual From the FTC," ACT | The App Association Blog, (Mar. 5, 2024), *available at* https://actonline.org/2024/03/05/killing-commerce-for-dummies-a-how-to-manual-from-the-ftc/.

[16] *Id.*

Sincerely,

Morgan Reed
President
ACT | The App Association