“Congress Should Enact a National, Comprehensive Consumer Privacy Framework”

Testimony of

Maureen K. Ohlhausen

Former Acting Chair of the Federal Trade Commission

Senate Committee on Commerce, Science, and Transportation

September 29, 2021

Chair Cantwell, Ranking Member Wicker, and other distinguished Members of this Committee, thank you for the opportunity to testify at this important hearing examining how to better protect consumer privacy. My name is Maureen Ohlhausen, and I am a partner at the law firm Baker Botts L.L.P. I had the pleasure of serving as an FTC Commissioner (2012–2018) and Acting Chairman (2017–2018).

The FTC is our nation's leading consumer privacy protection agency. It has brought hundreds of privacy- and data security-related enforcement actions, covering both on- and offline practices and fast-evolving technologies.[1] The FTC has creatively used every enforcement, policy, and educational tool at its disposal in its privacy and data security work to protect consumers' personal information, while still allowing consumers to enjoy the benefits of the many innovative products offered in today's dynamic marketplace. However, as the collection, use, and sharing of personal data have continued to grow in amount and complexity, consumers and businesses are now required to navigate a tangled web of confusing, and often inconsistent, data privacy requirements from various levels of government, and from various nations and regions throughout the world.

While I am proud of the FTC's privacy and data security enforcement efforts, the agency currently operates under several material constraints that limit the FTC's effectiveness absent further action by Congress. You and your colleagues can remove these constraints by enacting comprehensive, technology neutral, national privacy legislation that provides clear protections for

[1] *See, e.g.*, FED. TRADE COMM'N, FTC'S USE OF ITS AUTHORITIES TO PROTECT CONSUMER PRIVACY AND SECURITY (2020), https://www.ftc.gov/system/files/documents/reports/reports-response-senate-appropriations-committee-report-116-111-ftcs-use-its-authorities-resources/p065404reportprivacydatasecurity.pdf; *Oversight of the Federal Trade Commission: Strengthening Protections for American's Privacy and Data Security: Hearing Before the S. Comm. on Commerce, Science, and Transportation*, 116th Congress (2019-2020) (statement of the FTC), https://www.ftc.gov/system/files/documents/public_statements/1578963/p180101testimonyftcoversight20200805.pdf.

consumers, articulates specific limits on companies' ability to collect, use, and share sensitive personal information, and grants the FTC the resources and explicit authority necessary to enforce a new law.

I would like to address what I view as reasons why reliance on the FTC's current authority cannot provide the same benefits as a federal privacy law. First, with the exception of discrete areas such as children's privacy and fair credit reporting, the FTC lacks explicit authority to enforce statutory privacy requirements or promulgate privacy regulations. Section 5 of the FTC Act gives the agency the authority to prevent certain entities from "using … unfair or deceptive acts or practices in or affecting commerce" ("UDAP"). This language has rightly been interpreted to permit the FTC to police unfair or deceptive privacy and data security practices, but it does not provide the clear statutory guidance found in other laws. For example, under the Fair Credit Reporting Act, the FTC can impose affirmative obligations on entities to provide rights of access to and correction of data. These rights would also be available under federal privacy legislation introduced by Members of this Committee. But the FTC likely could not impose such obligations based on its UDAP authority alone.

Second, the FTC's ability to promulgate rules under its broad UDAP authority is governed by a special process in the Magnuson-Moss Warranty-Federal Trade Commission Improvement Act. Congress set up this process specifically to cabin the agency's broad UDAP authority by imposing additional procedural requirements and other protections.[2] By contrast, where Congress has provided the agency with detailed statutory guidance on subject matter and goals, it has

[2] Magnuson-Moss Warranty—Federal Trade Commission Improvement Act, Pub. L. No. 93–637, § 202, 88 Stat. 2183, 2193 (1975) (codified as amended at 15 U.S.C. §§ 45–46, 49–52, 56–57c, 2301–2312 (2012)); 15 U.S.C. § 57a(a)(1)(B).

expressly permitted the FTC to use Administrative Procedure Act notice-and-comment rulemaking, and specifically exempted the agency from the additional procedures of Magnuson-Moss rulemaking.

Third, an FTC rulemaking under existing authority may not necessarily preempt state laws. If the FTC does not preempt state laws, this would permit the continued proliferation of disparate state requirements, and would make a coherent, consistent national framework nearly impossible. In addition, there will inevitably be a conflict between an FTC rulemaking and the increasing number of state laws and rulemakings, which will create confusion with respect to what requirements apply, and will further fragment U.S. privacy protections.

Simply put, the FTC's existing framework is not conducive to adopting comprehensive, national consumer privacy and data security requirements in a manner that can provide the clarity and certainty consumers and businesses seek. That is why I respectfully request that Congress turn its focus back to enacting privacy legislation.

Last year, I testified before this committee in support of Congressional efforts to enact comprehensive federal privacy legislation. The events of the past year make the need for such legislation even more apparent. Due to the COVID-19 pandemic, we have seen a rapid shift to online work and learning, as well as the deployment of technological efforts to track the path of the virus. The California Consumer Privacy Act ("CCPA") went into effect in 2020, but the landscape continues to shift, as California's ballot initiative (the California Privacy Rights Act) amended the CCPA, and Virginia and Colorado enacted their own consumer privacy laws.

These developments reinforce the need for federal action. Congress needs to act quickly, and I urge the Leadership and Members of this Committee to continue to take important steps in that direction.

I realize that there are still points of contention with respect to privacy legislation. However, what we all have in common is a desire for clear consumer privacy protections that apply throughout the nation based on the sensitivity of the data, and which allow consumers to continue to benefit from innovative technologies, such as those we have come to rely on even more heavily during this pandemic. We want consumers to enjoy confidence that their personal information is not subject to varying protections within a state or from state to state, regardless of the entity that collects such information, based on the sensitivity of the data and how it is used.[3]

I support strong consumer privacy rights and believe firmly in providing transparency and control to consumers, robust security, and strong accountability as outlined in the FTC's bipartisan 2012 landmark Privacy Report.[4] Further, as someone who has also focused on the intersection of antitrust and privacy law, and the impact of regulation of market competition, I urge that a federal

[3] *See* Memorandum from Public Opinion Strategies and Peter D. Hart to the Progressive Policy Institute, Key Findings from Recent National Survey of Internet Users (May 26, 2016), https://www.progressivepolicy.org/wp-content/uploads/2016/05/Internet-User-National-Survey-May-23- 25-Key-Findings-Memo.pdf (finding that 94% of consumers favor such a consistent and technology-neutral privacy regime, and that 83% of consumers say their online privacy should be protected based on the sensitivity of their online data, rather than by the type of Internet company that uses their data). *See also* https://www.progressivepolicy.org/press/press-releases/press-release-consumers-want-one-set-rulesprotecting- information/ ("Ultimately, consumers want to know there is one set of rules that equally applies to every company that is able to obtain and share their data, whether it be search engines, social networks, or ISPs, and they want that data protected based on the sensitivity of what is being collected' said Peter Hart.").

[4] *See* FED. TRADE COMM'N, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE: RECOMMENDATIONS FOR BUSINESSES AND POLICYMAKERS (2012), https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf.

approach be technology-neutral and avoid unduly burdening smaller entities, innovative services, or certain entities in the internet ecosystem.

Key Elements of an Effective Federal Framework

I strongly believe that Congress needs to enact federal privacy legislation that includes several key attributes. First, legislation should provide a national and uniform set of protections and consumer rights throughout our digital economy. Second, it should ensure strong enforcement that protects consumer information that could result in harm if disclosed or misused, while also allowing companies to provide and develop innovative products and services that consumers want. Third, it should provide consumers clarity and visibility into companies' data collection, use, and sharing practices, as well as easily understandable choices regarding these practices, calibrated to the sensitivity of that data. Fourth, legislation should be more comprehensive than current state laws, such as the CCPA, addressing more elements of the data cycle. Fifth, federal privacy legislation should be enforced by the FTC, which has the experience and skill to meaningfully enforce a new law's protections, supplemented by state attorneys general ("AGs").

1. Provide a national and uniform set of protections and consumer rights

Federal legislation should be technology-neutral and apply to all entities across the internet ecosystem that collect, share, or make use of consumer data, whether they are technology companies, broadband providers, or retailers. What matters is not who collects the data, but what data is collected, how sensitive it is, and how it is protected and used.

Strong privacy protections need to apply to consumers regardless of where in the United States they live, work, or happen to be accessing information. By its very nature, the Internet

connects individuals across state lines. Data (and, increasingly, commerce) knows no state boundaries. For this reason, a proliferation of different state privacy requirements creates inconsistent and confusing privacy protections for consumers, as well as significant compliance and operational challenges for businesses of all sizes. Although privacy regulation is often justified by concerns about big online players having large amounts of consumer information, regulatory complexity actually works to favor large, established companies.[5] It also erects barriers to the kind of innovation and investment that is a lifeblood of our nation's economy and to many beneficial and consumer-friendly uses of information.

2. *Protect consumer information that could result in harm if disclosed or misused*

A federal privacy law should protect individuals' information, the use or disclosure of which could result in harm. Accordingly, such legislation should cover data that identifies an individual, whereas data that does not identify an individual poses a minimal risk of harm and need not be subject to the same requirements.

Sensitive personal information, such as health and financial information, real-time precise geo-location information, social security numbers, and children's information, poses the highest risk of consumer harm and should be subject to the highest protections.[6] In turn, to mirror consumer expectations and preferences, there should be less-stringent requirements on non-sensitive personally identifiable information, reflecting the lower risk of consumer harm. Information that

[5] *See, e.g.*, Jian Jia, Ginger Zhe Jin, Liad Wagman, "The Short-Run Effects of GDPR on Technology Venture Investment"
(working paper, National Bureau of Economic Research, November 2018), https://www.nber.org/papers/w25248).
[6] These types of information reflect a general consensus, as recognized in the FTC's 2012 report, *supra* note 4 at 58–59. Other types of information may be sensitive, as reflected in consumer expectations.

is reasonably de-identified, aggregated, or publicly available does not raise the same specter of harm and falls outside the scope of necessary consumer protections.

3. ***Reflect consumer preferences through simple choices based on data sensitivity***

I believe that an optimal approach would balance ease of use and transparency by giving consumers clear and simple privacy choices based on the nature of the relevant information itself—its sensitivity and the correlated risk of consumer harm if such information is the subject of an unauthorized disclosure. A federal privacy law should promote consumer control and choice by imposing requirements for obtaining meaningful consent based on the risks associated with different kinds and uses of consumer data.

As I discussed earlier, sensitive data should be afforded stronger protections under a federal privacy law than non-sensitive personally identifiable data and non-identifiable information. In line with this concept, the most sensitive data should be subject to an opt-in consent requirement, while other personally identifiable covered data would be suitably protected by opt-out consent. Further, for certain types of routine operational uses, such as order fulfillment, fraud prevention, network management, and some forms of first-party marketing, consent should be inferred, consistent with consumer expectations.

4. ***Legislation should be more comprehensive than current state laws***

Federal privacy legislation should address gaps and shortcomings of current privacy laws. A strong federal privacy law should build on elements of current efforts in California, Virginia, and Colorado, and include safeguards protecting uses of consumer data throughout the United States.

5. ***Ensure strong accountability and enforcement that best protects consumer interests***

The Members of this Committee recognize that Congress must develop a law that guarantees strong privacy rights to consumers and adopts best practices from state laws, while creating uniformity across the nation. But preempting state laws should not mean weakening protections for consumers. A federal privacy law needs to be a strong one. I believe that states, as well as the FTC, have a critical role to play in protecting and enforcing those rights.

The FTC should have the primary authority to enforce a national privacy law. The FTC is already protecting consumer privacy, making it experienced and knowledgeable in the field. Moreover, it is well-equipped to assess the interaction between competition and privacy law in the United States. Congress should make use of these existing strengths, rather than start from scratch with a newly-formed, and inexperienced, agency.

Federal privacy legislation should support strong enforcement by the FTC, allowing the agency to obtain meaningful results. Rather than being limited to violations of previous orders, the FTC needs to be able to fine companies for first-time violations of a new, comprehensive privacy law to provide sufficient incentives for companies to take the necessary steps to ensure responsible use and protection of consumer data.

However, as I discussed earlier, as privacy concerns become weightier and more complex, the FTC is reaching the limits of its current tools—which it has made clear in its statements,

including those made before the Committee.[7] Congress must provide the FTC with greater statutory clarity coupled with more resources to protect consumer privacy in America.

Despite the ever-growing need for privacy enforcement, the FTC's budget has been flat since 2013. The number of full-time employees lags behind where it was in the early 1980s and comparable bodies tasked with data protection.[8] Meanwhile, the Internet and the collection, use, and sharing of consumer data have grown enormously. I urge Congress to address that widening gap to meaningfully support an issue as important and complicated as consumer privacy.

I recognize that state AGs are critical allies in the realm of consumer protection. They should be given the power to enforce any new federal law, taking on violations that the FTC is yet to investigate or that have a particular impact in their respective state. By working in unison, the FTC and state AGs can create an efficient process that reduces duplicative matters and supports consistency for all consumers.

A federal privacy law, though, should not include private rights of action with statutory or punitive damages. These approaches often result in class actions that primarily benefit attorneys, while providing little, if any, relief to those who are harmed. Private rights of action may also lead to abuses, such as frivolous assertions and attempts to seek "nuisance fee" settlements. This results in the diversion of company resources from compliance to litigation, which ultimately does not help consumers who, at the end of the day, simply want companies to follow the law. Like state

[7] *See, e.g.*, FED. TRADE COMM'N, FTC REPORT ON RESOURCES USED AND NEEDED FOR PROTECTING CONSUMER PRIVACY AND SECURITY (2020), https://www.ftc.gov/system/files/documents/reports/reports-response-senate-appropriations-committee-report-116-111-ftcs-use-its-authorities-resources/p065404reportresourcesprivacydatasecurity.pdf; *Oversight of the Federal Trade Commission*, *supra* note 1 at ("Section 5, which we use to bring our general privacy and data security cases, is not without its limitations.").

[8] *Id*. at 2–3.

law preemption, trusting enforcement to the FTC and state AGs fosters consistency, and is ultimately more beneficial to consumers.

Providing the FTC and state AGs with clear privacy protections, backed up with strong enforcement authority and expanded resources, represents a highly beneficial approach for consumers, as evidenced by the successful and bipartisan work in policing violations of children's privacy through the Children's Online Privacy Protection Act. Providing the FTC with enhanced authority to facilitate consumer redress for privacy violations would also ensure that consumers can be compensated directly and promptly when companies engage in harmful data practices.

Conclusion

Thank you again for the opportunity to testify today. I look forward to working with all Members of the Committee and all stakeholders in crafting strong national privacy legislation.