

“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 23, 2020

Chairman Wicker, Ranking Member Cantwell, and other distinguished Members of this Committee, thank you for the opportunity to testify at this important hearing examining legislative proposals to protect consumer data privacy and provide baseline data protections for all Americans. 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 a Commissioner (2012–2018) and Acting Chairman (2017–2018) of our nation’s leading consumer privacy protection agency, the Federal Trade Commission (“FTC”). I am testifying today in my capacity as a former FTC official.

The FTC has brought hundreds of privacy- and data security-related enforcement actions, covering both on- and offline practices and fast-evolving technologies.¹ It 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 regulations from various levels of government.

Last year, I testified before this committee in support of Congressional efforts to enact comprehensive federal privacy legislation. The events of 2020 make the need for such legislation even more apparent. Due to the COVID-19 pandemic, we have seen a rapid shift to online work

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.

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 earlier this year but the landscape continues to shift, as California and other states consider additional law and regulations. All of these developments reinforce the need for federal action. I therefore commend the Members of this Committee for your ongoing leadership in releasing proposed federal privacy legislation to give stronger protections to consumers, impart clearer guidance to businesses coupled with more accountability, and provide more authority to the FTC to police harmful data practices. Congress needs to act quickly, and the Leadership and Members of this Committee today continue to take very important steps in that direction.

What we all have in common is a desire for there to be 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 period. We want consumers to enjoy confidence that their personal information has the same protections within a state or from state to state, regardless of the entity that collects such information, based on the sensitivity of the data.² As noted above, such concerns have become even more prominent in recent months in light of the COVID-19 pandemic.³

² 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.”).

³ See, e.g., *Enlisting Big Data in the Fight Against Coronavirus Hearing Before the S. Comm. on Commerce, Science, and Transportation*, 116th Congress (2019-2020),

I am a supporter of 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 approach be technology neutral and avoid unduly burdening smaller entities or innovative services.

Key Elements of an Effective Federal Framework

I strongly believe that Congress needs to enact federal privacy legislation that includes several key attributes. Legislation should provide a national and uniform set of protections and consumer rights throughout our digital economy. 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. Any privacy law 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. Legislation should be more comprehensive than current state laws, such as the CCPA, addressing more elements of the data cycle. Finally, federal privacy legislation

<https://www.commerce.senate.gov/2020/4/enlisting-big-data-in-the-fight-against-coronavirus> (examining “how consumers’ privacy rights are being protected and what the U.S. government plans to do with COVID-related data”); *How Americans See Digital Privacy Issues Amid the COVID-19 Outbreak*, PEW RESEARCH CTR. (May 4, 2020), <https://www.pewresearch.org/fact-tank/2020/05/04/how-americans-see-digital-privacy-issues-amid-the-covid-19-outbreak/> (surveying trends in American views on privacy).

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>.

should be enforced by the FTC, who has the experience and skill to meaningfully enforce the new law's protections, supplemented by state attorneys general.

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 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. Put simply, data (and, increasingly, commerce) knows no state boundaries. For this reason, a proliferation of different state privacy requirements would create inconsistent 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 the favor of large, established companies and hampers smaller entities.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

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>).

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 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 reflect 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 is reasonably de-identified, aggregated, or publicly available does not raise the same specter of harm and warrants different treatment.

3. Legislation should be more comprehensive than current state laws

Federal privacy legislation should address gaps and shortcomings of current privacy laws. While the CCPA is a commendable effort for protecting consumer privacy, it primarily applies to the sharing, disclosure, and subject access rights of data.⁷ Similarly, the CCPA requires an opt-in for sharing children's information, but does not impose the same restriction for using that data.⁸ A strong federal privacy law should build on elements of current efforts and include safeguards protecting uses of consumer data.

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.

⁷ *See, e.g.*, CAL. CIV. CODE §§ 1798.100, .105, .110, .115 (focusing on businesses that collect or sell personal information).

⁸ *See* CAL. CIV. CODE § 1798.120(c).

4. 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 discussed above, 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.

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. Congress should make use of this existing strength, 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 the 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 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 Committee.⁹ Congress must provide the FTC 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.¹⁰ 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.

⁹ 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.”).

¹⁰ *Id.* at 2–3.

I recognize that state attorneys general (“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—and may choose to intervene in, if needed. 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 to obtain monetary redress or statutory penalties. These approaches often result in class actions that primarily benefit attorneys, while providing little, if any, relief to those who were 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 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 enforcement power, 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 (“COPPA”). Providing the FTC with enhanced authority to provide consumer redress 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, and

I applaud the Committee's Leadership and other Members for releasing drafts that will provide the foundation for Congressional action.

The United States would benefit significantly from a strong and unified, technology- and industry-neutral federal privacy law that applies uniformly to all entities, regardless of their business model. A new federal law that preempts state laws would provide both consumers and businesses with necessary guidance and give consumers much-needed control over their data. Such a federal law would provide the greatest clarity and certainty about the rights of consumers, as well as the responsibilities of companies that collect, use, or share consumers' personal information.

That is why a new law, backed up by an experienced and expert agency like the FTC—one with expanded powers and resources—is the best hope for consumers when it comes to meaningful privacy protections.