"Congress Needs to Enact a National, Comprehensive Consumer Privacy Framework"

Testimony of

Maureen K. Ohlhausen

Co-Chair, 21st Century Privacy Coalition

Senate Committee on Commerce, Science, and Transportation

December 4, 2019

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. My name is Maureen Ohlhausen, and I am a partner at the law firm Baker Botts L.L.P. Along with Jon Leibowitz, I also serve as co-chair of the 21st Century Privacy Coalition (Coalition).[1] 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).

The FTC has brought hundreds of privacy- and data security-related enforcement actions, covering both on- and offline practices and fast-evolving technologies.[2] 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, and consumers and businesses are increasingly required to navigate a tangled web of confusing, and often inconsistent, data privacy regulations from various levels of government, the Coalition believes it is imperative that Congress enact comprehensive federal privacy legislation. We therefore commend the Members of this Committee for your 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. To avoid a patchwork of inconsistent, even

[1] The 21st Century Privacy Coalition is comprised of the nation's leading communications providers and their trade associations, including AT&T, CenturyLink, Comcast, Cox Communications, CTIA, NCTA – The Internet and Television Association, T-Mobile, USTelecom, and Verizon.

[2] *See, e.g.*, FTC 2018 Privacy and Data Security Update, https://www.ftc.gov/system/files/documents/reports/privacy-data-security-update-2018/2018-privacy-data-security-report-508.pdf.

conflicting, privacy requirements, Congress needs to act quickly, and the Leadership and Members of this Committee today take a very important step in that direction.

The Coalition is part of a strong consensus among businesses, civil society groups, and consumers in support of federal privacy legislation. As an extensive survey by the Progressive Policy Institute conclusively found, consumers (1) overwhelmingly (i.e., 94%) want the same privacy protections to apply to their personal information *regardless* of the entity that collects such information and (2) overwhelmingly (83%) expect to enjoy heightened privacy protections for sensitive information and for uses of their sensitive information that present heightened risk of consumer harm, again *regardless* of the company charged with maintaining it.[3]

What we all have in common is a desire for there to be clear consumer privacy protections that apply throughout the nation, no matter where you live, work, or travel. We want consumers to enjoy confidence that their personal information is not subject to different protections within a state or from state to state. We are supporters 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]

---

[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* FTC Report, Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers (Mar. 2012), available at https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protectingconsumer- privacy-era-rapid-change-recommendations/120326privacyreport.pdf.

Key Elements of an Effective Federal Framework

We strongly believe that Congress needs to enact federal privacy legislation that includes three key attributes. First, it should provide consumers clarity and visibility into companies' data collection, use, and sharing practices, as well as choices regarding these practices, calibrated to the sensitivity of that data. Second, legislation should provide a national and uniform set of protections and consumer rights throughout our digital economy. Third, it should ensure strong enforcement that protects consumer from harmful data practices, while also allowing companies to provide and develop innovative products and services that consumers want.

1. *Reflect consumer preferences through simple choices based on the sensitivity of data*

We 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 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. We also believe that consumers should have certain rights of access, correction, and deletion where appropriate.

So-called sensitive personal information, such as health and financial information, real-time geo-location information, social security numbers, and children's information, should be subject to the highest protections. In turn, to reflect consumer expectations and preferences, there should be less-stringent requirements on *non*-sensitive personal information, as well as information that is de-identified or aggregated because such information has a lower risk of consumer harm or association with a particular individual. And, for certain types of routine operational uses, consent should be inferred. As recognized by the FTC in its 2012 Report, these

uses, which include order fulfillment, fraud prevention, network management, and some forms of first-party marketing, are expected by consumers and provide them a variety of benefits, including knowing about promotions and discounts tailored to their existing services and products.

Striking the right balance in categorizing data as sensitive or non-sensitive is crucial for consumers and essential for an effective privacy law. A regime that requires consumers to constantly provide consent for data collection and uses that are expected and raise little risk of substantial harm will not only impose unnecessary burdens on consumers (as well as businesses), but will also reduce consumers' focus on the affirmative consent requests for the types of sensitive data whose misuse may lead to more serious consequences.

A federal privacy law must also recognize that consumers have a wide variety of preferences about the benefits of sharing their personal data. Legislation should not limit consumer choice by, for example, inhibiting consumer-friendly incentive programs tied to privacy choices, such as rewards or loyalty programs. Rather, the law should require that companies give consumers clear and comprehensible information about the categories of data that are being collected, used, or shared, and the types of third parties with which information may be shared. So long as consumers are provided with clear information about the nature of such programs, they should be allowed to make their own choices, especially because such programs often involve significant cost savings and other benefits to consumers.

2. *Provide a national and uniform set of protections and consumer rights throughout our digital economy*

As discussed above, a new federal privacy law should provide meaningful consumer control and choice over consumers' personal data based on the sensitivity of such information. Such 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, state intervention in this quintessentially interstate issue is problematic, no matter how well intentioned it may be. 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. 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. Indeed, even the authors of California's 2018 privacy law recognized the wisdom of preempting municipal privacy laws.

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

3. *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 consumer privacy law needs to be a strong one. The Coalition believes 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. As privacy concerns become weightier and more complex, the FTC is reaching the limits of its current tools. Under its existing legal regime, in which the FTC polices privacy under its Section 5 authority to

prevent unfair and deceptive acts or practices, when the FTC goes after a company for an initial privacy violation, it can require the company to change its practices through a consent order. In very limited circumstances, the FTC can obtain (non-punitive) monetary redress for consumers if the agency can show direct consumer losses. Only if a company later violates that order—and a judge agrees there has been such a violation—can the FTC impose a financial penalty (as opposed to obtaining consumer redress).

We believe 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. In certain cases, Congress should also give the Commission the authority to issue rules to fill in gaps in the law and to keep up with developments in technology. These rules will add clarity to the law so that companies understand what kind of behavior is out of bounds as technology and business practices evolve.

Congress must also 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—nearly four decades ago, when the phrase "big data" meant an encyclopedia and the United States had one hundred million fewer people. The Internet and the collection, use, and sharing of consumer data have grown enormously without a similar boost in FTC resources. We urge Congress to address that widening gap if we are serious about tackling an issue as important and complicated as consumer privacy.

We also 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. A consumer privacy law, though, should not include private rights of action, which often result in class actions

that primarily benefit attorneys while providing little, if any, relief to actual victims. Private rights of action also frequently result 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. Nor would it be appropriate to ban pre-dispute arbitration clauses in the context of a new privacy law.

Providing the FTC and state AGs with enforcement power, backed up with civil fining authority and expanded resources, represents a far better 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 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. The Coalition looks forward to working with all Members of the Committee and all stakeholders in crafting strong national privacy legislation, and we 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.