Hearing on "Legislative Solutions to Protect Kids Online and Ensure Americans Data Privacy Rights"

Testimony of

Maureen K. Ohlhausen

Co-Chair, 21st Century Privacy Coalition

House Committee on Energy & Commerce

Subcommittee on Innovation, Data, and Commerce

April 17, 2024

Introduction

Chair Bilirakis, Ranking Member Schakowsky, Chair McMorris Rodgers, Ranking Member Pallone, and other distinguished Members of the subcommittee, thank you for the opportunity to testify at this important hearing examining legislative solutions to protect kids online and ensure Americans' data privacy rights. My name is Maureen Ohlhausen, and I am co-chair of the 21st Century Privacy Coalition ("Coalition"),[1] as well as a partner at the law firm Wilson Sonsini. I had the honor of serving as a Federal Trade Commission ("FTC") Commissioner (2012–2018) and Acting Chairman (2017–2018). I am testifying today on behalf of the Coalition.

I would like to begin by commending Chair McMorris Rodgers and Senate Commerce Chair Cantwell for the release of the American Privacy Rights Act discussion draft. The Coalition has advocated for comprehensive national privacy legislation for a decade, and we have always believed that such legislation needs to be bipartisan to be successful. This discussion draft shows that there is potential for a bipartisan path forward on this urgently needed legislation.

The Coalition appreciates that many Members of Congress are committed to enacting federal privacy legislation. All of us share a desire for strong consumer privacy protections that apply uniformly throughout the nation based on the sensitivity and use of the data, and which allow consumers to continue to benefit from services and technologies on which we have come to rely. We want consumers to have confidence that their personal information is not subject to varying protections from state to state, or even within a state, regardless of the entity that collects such

[1] The member companies/associations of the 21st Century Privacy Coalition are AT&T, Comcast, Cox Communications, CTIA, DIRECTV, T-Mobile, and USTelecom,.

information.[2] Federal legislation should also provide strong enforcement that protects consumer data that could result in harm if misused or disclosed, while also allowing companies the flexibility to develop innovative new products that consumers want.

The Discussion Draft Has Many of the Elements Necessary for a National Privacy Framework

The discussion draft incorporates a number of elements that are foundational in privacy legislation. First, it is strong and comprehensive, addressing issues such as transparency; consent and other consumer rights; data security; and the relationship between companies, their vendors, and third parties. Second, the legislation designates the FTC as the federal agency responsible for enforcing the new law, and permits State Attorneys General to assist the FTC with its enforcement.

Third, as the former Acting Chair of the FTC, I am particularly appreciative that this draft provides the FTC with several useful enforcement tools, such as civil penalty authority for a first violation of the legislation, limited APA rulemaking authority, the ability to provide restitution to consumers harmed by violations, and jurisdiction over common carriers. The FTC has brought hundreds of privacy- and data security-related enforcement actions, covering both on- and offline

[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.").

practices and fast-evolving technologies,[3] and is well-suited to draw on its experience and knowledge in the field to vigorously enforce the law, while still allowing consumers to enjoy the benefits of the many innovative products offered in today's dynamic marketplace. This legislation would empower the FTC with more-effective enforcement tools to protect consumers from privacy harms, though such tools should be accompanied by appropriate guardrails to ensure that the FTC does not exceed its authority. In addition, we appreciate that the discussion draft would terminate the FTC's commercial surveillance proceeding.

Fourth, the discussion draft provides a national privacy and data security framework that generally preempts state laws and regulations. In the absence of such a framework, consumers and businesses today are required to navigate a tangled web of confusing, and often inconsistent, data privacy requirements from various levels of government. American consumers and businesses deserve the clarity and certainty of a single federal standard for privacy. That is why state preemption must be an essential component of national legislation.

Fifth, the discussion draft recognizes not only that the FTC is the federal agency with the greatest expertise to enforce this new law, but that legacy privacy requirements in the Communications Act must be preempted. This would allow the FTC to take a holistic and modern approach to protecting consumer privacy based upon the type of information collected,

[3] *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.

used, or shared, rather than the legacy regulatory history of the entity collecting, using, or sharing such information.

Areas In Which the Discussion Draft Needs Improvement

We believe, however, that the discussion draft needs to be improved before this subcommittee or the Energy & Commerce Committee takes any additional action on the legislation. The draft raises several concerns that warrant further consideration. First, although the draft would preempt the Federal Communications Commission's ("FCC") privacy and data security authority, it stops short at preempting the FCC's data breach notification authority.

The FCC's recent data breach order, adopted on a 3-2 vote, demonstrates that the FCC lacks the expertise to impose requirements in this area, and that it is willing to overstep its authority and ignore Congress's clear direction. The FCC also adopted data breach rules that are inconsistent with the requirements of other federal agencies, making the case yet more compelling that the FCC's authority should be eliminated and replaced with a holistic approach to enforcing the bill's privacy and data security requirements.

Second, the draft appropriately seeks to replace the Communications Act's provisions addressing video privacy requirements with equivalent protections that would be enforced by the FTC. We appreciate the draft's goal of porting the structure of Sections 631 and 338(i) of the Communications Act and the Video Privacy Protection Act ("VPPA") into the draft in order to allow the operational practices that have arisen around the use of viewing information, which have balanced the need to protect privacy and prevent unwanted disclosure of such information with the benefits of fostering innovation and new features and services for video customers. However, the language included in the bill is a departure from the language marked up by this committee in

2022, and we believe this new draft language could unintentionally cause significant disruption to operational, marketing, and advertising practices that have long served consumers well in the television marketplace. In addition, defining general communications usage and billing data as sensitive changes the regulatory structure that has governed such data for decades.

Some modest tweaks to the draft could address these concerns. Given the authority that the FTC would have over the privacy of video programming information, Congress should also clarify that the VPPA does not apply to entities subject to the bill's requirements.

Third, the bill should be refined so it better reflects a risk-based approach based on the nature of the relevant information and how it is used. This would be consistent with well-established principles of privacy laws and the FTC's privacy enforcement practices. We are concerned that the bill creates uncertainty for routine operational uses of information that are necessary to serve customers and operate a business. The framework of the draft requires all such operational uses of data to fit within one of the 15 statutory permissible purposes, while imposing overly restrictive standards on activities such as internal research and first-party marketing. For example, our companies provide a suite of communications services, often in a bundled package. Our customers benefit when we are able to use information we collect in the course of serving them to enhance such services, and to market our other services, packages, or pricing that better suit their needs.

While we appreciate that first-party marketing is included as a purpose for which data can be collected and used, we are concerned that sensitive information is not included in this exception to the bill's data minimization requirement. Given how broadly the discussion draft defines sensitive data, the legislation would undermine the ability of communications providers to tailor

products and pricing to existing customers based upon how they use our services. In addition, we think that interest-based advertising, which involves the delivery of advertisements based upon our customers' consumption of our services, should be included as a permissible purpose along with first-party marketing and contextual advertising. It is also not clear whether product improvement is a permissible purpose if such improvement is done by using data that is not de-identified.

Fourth, the draft seemingly provides broad state preemption, but includes a number of exceptions to such preemption that may unduly limit its application. The failure to preempt these laws could enable plaintiffs to re-fashion privacy claims in a manner that circumvents the bill's stated purpose to "establish a uniform national data privacy and data security standard in the United States to prevent administrative costs and burdens placed on interstate commerce." In past hearings before Congress, witnesses from industry, academia, and civil society have urged the adoption of a national privacy standard that would prevent an inconsistent patchwork of state regulation. [4]

Establishing a truly national framework must be a core component of federal privacy legislation. Permitting states to adopt privacy-specific laws even after this law passes would be highly problematic, as would allowing plaintiffs to invoke broad types of claims to circumvent the

[4] *See Protecting Consumer Privacy in the Era of Big Data: Hearing Before the Subcomm. on Consumer Protection & Commerce of the Comm. on Energy & Commerce*, 116th Cong. (2019) (statement of David F. Grimaldi, Jr., Exec. Vice President, Public Policy, Interactive Advertising Bureau) (stating a privacy framework should "reduce consumer and business confusion by preempting the growing patchwork of state privacy laws"); *id.* (statement of Roslyn Layton, Visiting Scholar, American Enterprise Inst.) (calling for a "single standard of data protection" and a "technology neutral national framework with a consistent application across enterprises."); *id.* (statement of Denise E. Zheng, Vice President, Tech. & Innovation, Business Roundtable) ("Legislation should eliminate fragmentation of privacy protections in the United States by harmonizing approaches to consumer privacy across federal and state jurisdictions through a comprehensive national law that ensures consistent privacy protections and avoids a state-by-state approach that leads to consumer confusion and makes compliance nationwide very challenging."). Additionally, testimony from Nuala O'Connor, then CEO of the Center for Democracy and Technology, described CDT's model baseline privacy legislation, which includes preemption of state privacy laws. *See* Center for Democracy & Tech., Federal Baseline Privacy Legislation Discussion Draft (Dec. 5, 2018), https://cdt.org/wp-content/uploads/2018/12/2018-12-12-CDT-Privacy-Discussion-Draft-Final.pdf.

bill's prohibition on privacy-specific laws. The predictable outcome would lead to confusion and litigation, both of which the legislation should strive to avoid.

Fifth, the discussion draft would abrogate arbitration agreements while inviting harmful class-action lawsuits that would undermine, not bolster, compliance with the legislation by adopting an overly broad definition of the term "substantial privacy harm." The unavailability of pre-dispute arbitration agreements if a plaintiff even alleges a substantial privacy harm would potentially permit plaintiff's lawyers to file frivolous lawsuits rather than allow consumers to bring such claims in arbitration, which is often a faster and more efficient way of resolving disputes.. In addition, the discussion draft would not prohibit class action lawsuits or class arbitrations, which would give the plaintiff's bar a financial incentive to bring frivolous claims. Even more concerning, the discussion draft lacks a delay of the availability of the private right of action, but includes an accelerated six-month implementation deadline. Coupled with the extremely limited right to cure before litigation can be initiated, the draft would seem to subject businesses to frivolous litigation and provide a windfall to the plaintiff's bar.

Conclusion

Thank you again for the opportunity to participate in today's hearing. We view this draft as progress toward developing a comprehensive national privacy law, but also believe improvements are necessary to achieve the draft's underlying purposes.

It is critical that Congress enact privacy legislation this year to address the growing patchwork of state laws, though we also urge the Committee to keep working to improve the bill, especially in the areas I have addressed in my testimony. The Coalition appreciates the opportunity to continue to work with the Committee to achieve bipartisan consensus on national, technology-

neutral privacy legislation that provides clear protections for consumers, while not undermining innovative and consumer-enhancing uses of data. I look forward to your questions.