Hearing on "Protecting America's Consumers: Bipartisan Legislation to Strengthen Data Privacy and Security"

Testimony of

Maureen K. Ohlhausen

Co-Chair, 21st Century Privacy Coalition

House Committee on Energy & Commerce

Subcommittee on Consumer Protection and Consumer

June 14, 2022

Introduction

Chair Schakowsky, Ranking Member Bilirakis, Chair Pallone, Ranking Member McMorris Rodgers, and other distinguished Members of the subcommittee, 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 co-chair of the 21st Century Privacy Coalition ("Coalition"),[1] as well as a partner at the law firm Baker Botts L.L.P. I had the pleasure 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 the authors of the bipartisan, bicameral discussion draft that is the subject of today's hearing. The Coalition has advocated for comprehensive national privacy legislation for nearly 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 the authors and many Members of Congress are committed to enacting federal 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 even more heavily during this pandemic. We want consumers to enjoy confidence that their personal information is not subject to varying protections from state to state, or even within a state,

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

regardless of the entity that collects such 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 Legislation Has Many of the Elements Necessary for a National Privacy Framework

The discussion draft incorporates a number of elements that the Coalition perceives as foundational in privacy legislation. First, it is stronger and more comprehensive than existing state laws, addressing issues such as transparency; consent and other consumer rights; data security; civil rights protections; and the relationship between companies, their affiliates, their vendors, and third parties. Second, the legislation designates the FTC as the principal agency responsible for enforcing the new law, and permits State Attorneys General to assist the FTC with its enforcement.

As the former Acting Chair of the FTC, I am particularly appreciative that this draft also provides the FTC with several sorely-needed enforcement tools, such as civil penalty authority for a first violation of the Act, 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 violations.

Third, the discussion draft provides a national privacy and data security framework that preempts state laws, regulations, and other requirements. 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.

Fourth, the discussion draft at least partially recognizes not only that the FTC is the 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 more holistic and modern approach to protecting consumer privacy based upon the type of information collected, used, or shared, rather than the legacy regulatory history of the entity collecting, using, or sharing such information.

[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.

Areas In Which the Bill 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, though the draft would preempt the Federal Communications Commission's ("FCC") privacy and data security authority with respect to broadband and video services, it stops short at preempting the same authority with respect to voice services.

In today's converged, digital world, consumers utilize traditional voice services as well as over-the-top services and applications to engage in voice communications. Congress should provide a holistic set of requirements governing the privacy associated with voice-related information. It does not benefit consumers to impose different requirements that depend upon an entity's legacy regulatory history.

Second, while the bill appropriately seeks to replace the FCC's traditional oversight of video privacy requirements with equivalent protections that would be enforced by the FTC, the language used in the bill far exceeds the requirements of the Cable Act and equivalent satellite protections, as well as the reasonable obligations and standards incorporated into recent state privacy laws. The cable and satellite privacy requirements have worked well for over five decades to protect consumers, while also fostering innovation in new features and services for cable customers.

If not changed, the video provisions of the bill could result in significant disruption to operational, marketing, and advertising practices that have long served consumers well in the television marketplace. It is critical that Congress not upend the balanced structure and

requirements of the Cable Act and its satellite corollary. Some modest tweaks to the draft could achieve this important result.

The same is true for the inclusion of voice information in the bill. In addition to addressing the regulatory disparity in the treatment of voice service providers I mentioned earlier in my testimony, the bill's language needs to be revised to permit consumers to benefit from the high level of service and customized packages they have come to expect.

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. 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 market services, packages, or pricing that better suit their needs. Such first-party marketing should be included in Section 209's general exceptions.

Fourth, the draft ostensibly provides broad state preemption, but includes a number of exceptions to such preemption that may unduly limit its application. 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]

[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

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. In addition, we are concerned about the meaning of the term "electronic surveillance" in the context of this bill, which is undefined and could be interpreted by states very broadly. The predictable outcome would lead to confusion and litigation, both of which the legislation should strive to avoid.

Fifth, the discussion draft would ban joint-action waivers in arbitration agreements, which would have the practical effect of making arbitration unavailable to millions of consumers with individualized claims who lack the resources to pursue such claims in court.

Conclusion

Thank you again for the opportunity to participate in today's hearing. I again applaud the authors of this bill and both Commerce Committees for the hard work that has gone into developing a comprehensive national privacy law. We view this draft as progress toward that goal, but also believe improvements are necessary to achieve the bill'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

---

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.

to continue to work with the bill's authors and the Committee to achieve bipartisan consensus on national, technology-neutral privacy legislation that provides clear protections for consumers, articulates specific limits on companies' ability to collect, use, and share sensitive personal information, and grants the FTC the explicit authority necessary to enforce a new law. I look forward to your questions.