“America’s Privacy Moment: The Need For Strong Federal Privacy Protections That Give Consumers More Control Over Their Data”

Testimony of

Jon Leibowitz

Co-Chair, 21st Century Privacy Coalition

Senate Committee on Commerce, Science, and Transportation

February 27, 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 policy principles for a federal data privacy framework. My name is Jon Leibowitz and I am a partner at the law firm of Davis Polk & Wardwell LLP. I also serve as co-chair of the 21st Century Privacy Coalition. During my time in government, I served as a Democratic Commissioner (2004-2009) and Chairman (2009-2013) of our nation's leading consumer privacy enforcement agency, the Federal Trade Commission ("FTC").[1]

There is a growing consensus both inside the halls of Congress and across America that federal privacy legislation is necessary to bolster consumer confidence in the privacy practices of online services, which in turn is necessary to foster continued U.S. innovation and leadership in the Internet ecosystem and the broader information-based economy. For those reasons and because it is the right thing to do, members of the 21st Century Privacy Coalition enthusiastically support federal legislation that provides stronger and more meaningful privacy protections for American consumers. We also want to commend this Committee, particularly Chairman Wicker and Senators Blumenthal, Moran, and Schatz, for its leadership on this important issue of intense public concern.

The 21st Century Privacy Coalition is composed of the nation's leading communications companies, which have a significant interest in fortifying consumer trust in online services and confidence in the privacy and security of their personal

[1] The FTC has brought hundreds of privacy and data security cases, including many against companies for misusing or failing to reasonably protect consumer data, almost always with unanimous votes from its Commissioners.

information.[2] We are supporters of strong consumer privacy rights and firmly believe that companies must provide transparency to consumers, disclose what consumer data is being collected and how it is being used, manage consumer data in a responsible manner,[3] and be held accountable for honoring their commitments to consumers. For decades, our companies have adhered to enforceable, robust privacy principles through practices that safeguard consumer data based on the key tenets of the bipartisan FTC privacy regime as outlined in the Commission's landmark Privacy Report.[4] We continue to adhere to such policies today.

Companies like ours that have always had vigorous privacy programs in place know that a uniform national privacy law would be good for the Internet economy. Last month, the Government Accountability Office ("GAO"), based on a request by House Energy & Commerce Chairman Pallone, produced its own report encouraging Congress to consider enacting a comprehensive Internet privacy law.[5] Our members welcome legislation that requires all marketplace participants to start from a place of transparency, security, control, and rights for American consumers.

---

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

[3] The 21st Century Privacy Coalition has also long supported strong federal data security legislation. *See, e.g., Discussion Draft of H.R.__, Data Security and Breach Notification Act of 2015: Hearing Before the Subcomm. on Commerce, Manufacturing, & Trade of the H. Comm. on Energy & Commerce*, 114 Cong. 59-67 (2015) (statements of Jon Leibowitz, Co-chair, 21st Century Privacy Coalition).

[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-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf.

[5] *See* Government Accountability Office, Internet Privacy: Additional Federal Authority Could Enhance Consumer Protection and Provide Flexibility (Jan. 2019), available at: https://www.gao.gov/assets/700/696437.pdf, at 37.

A Federal Solution Is Critical

We strongly believe that Congress needs to enact national privacy legislation that gives consumers statutory rights to control how their personal information is used and shared; provides increased visibility into companies' practices when it comes to managing consumer data; and includes an opt-in consent regime for the use and sharing of customers' sensitive personally identifiable information—including health and financial information, precise geo-location information, social security numbers, and children's information—consistent with the framework articulated by the FTC in its Privacy Report. The recommendations in the Privacy Report, which were lauded by the privacy community for their muscular approach to consumer protection, were based on institutional expertise accrued over decades, through hundreds of cases brought by the FTC against companies to ensure privacy and security of consumer information, as well as from the input of dozens of stakeholders (including businesses, privacy advocates, and academics), and multiple consumer privacy and data security workshops.

The FTC also recognized—and we hope you would agree—that privacy should not be about *who* collects an individual's personal information, but rather should be about *what* information is collected and *how* it is protected and used. That is why we firmly believe that federal privacy legislation should be technology- and industry-neutral. Companies that collect, use, or share the same type of personal information should not be subject to different privacy requirements based on how they classify themselves in the marketplace. 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.[6]

The optimal approach would provide consumers with easy-to-understand privacy choices based upon the nature of the information itself—its sensitivity, and the risk of consumer harm if such information is the subject of an unauthorized disclosure—and the context in which it is collected. For example, consumers expect sensitive information about their medical histories, financial status, and Social Security numbers to receive heightened protection to ensure confidentiality. A sensitivity- and risk-based approach imposes less stringent requirements on *non*-sensitive information and information that is de-identified or anonymized because of the lower risk that consumers would be harmed, or even that such information could be associated with an individual.

Accordingly, a national privacy law based on the FTC's Privacy Report would best promote consumer control and choice by imposing requirements for obtaining meaningful consent based on the risks associated with different kinds of data and different uses of data. That approach should include clear consumer controls such as opt-in rights for sensitive information, opt-out rights for non-sensitive information, and inferred consent for certain types of operational uses of information by companies (such

[6] *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 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-rules-protecting-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.").

as in the case of order fulfillment, fraud prevention, and some forms of first-party marketing). We also believe that consumers should have certain rights of access and deletion where appropriate.

A privacy law must also recognize that different consumers have different privacy preferences. One of the most remarkable things about the Internet is that it allows us to tailor our use to our own needs and interests. We agree with the GAO that Congress must carefully consider the balance between the need for consumer privacy protections and companies' ability to provide and improve the services on which we have come to expect and depend.[7] Legislation should not limit consumer choice by inhibiting consumer-friendly incentive programs tied to privacy choices such as rewards programs. Rather, the law should require companies to have a privacy policy that gives 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 information about the nature of such programs, they should be allowed to make their own choices.

A Problematic Patchwork: Avoiding Inconsistent State Laws

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 (and international) lines. Put simply, data knows no state boundaries.

[7] GAO Report, at 38.

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. A Mississippi wireless customer visiting Connecticut should not have different privacy protections than a Connecticut wireless customer visiting Mississippi. Nor should a Kansas resident enjoy different privacy protections when at work just over the border on the Missouri side of Kansas City, or a Hawaii resident when traveling to any of the contiguous U.S. states.

Thus, the absence of a national privacy law yields inconsistent protections and consumer confusion about the scope of their privacy protections and the jurisdictions in which such protections apply. In addition, the proliferation of state and local consumer privacy laws in place of a national framework creates 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.

Ensuring Enforcement

But preempting state laws should not mean weakening protections for consumers. A federal consumer privacy law needs to be a strong one. We believe that the Members of this Committee understand that, and we encourage all stakeholders to come together to develop such a federal law. Blanket opposition to preemption of state legislation offers no protection to consumers. Congress should be able to develop a law that guarantees strong privacy rights to consumers in—and adopts the best practices from the laws of—

every state. And the Coalition believes states as well as the FTC have a critical role to play in enforcing those rights.

The FTC should have the primary authority to enforce a national privacy law. Our nation's top consumer protection agency has brought more than 500 cases to protect the privacy and security of consumer information, including those against large companies like Facebook, Google, Twitter, Uber, Dish Network, and others. To support the agency in its mission, Congress should provide the FTC with the ability to impose civil penalties on violators for first offenses. We also recognize that the FTC may have a role to play in developing rules to address certain details that Congress may not be able to tackle in the legislation itself, although the boundaries of any such authority should be clear in the legislative text. And we strongly support Congress providing the agency with additional resources necessary to undertake appropriate enforcement actions to keep all companies honest and compliant.

While we believe federal legislation, rather than a state-by-state approach, should be enacted to ensure consistent, understandable, and robust consumer privacy rights, we also recognize that state attorneys general are critical allies in the realm of consumer protection. They should also be given the power to enforce any new federal law.

A consumer privacy law, though, should not include criminal penalties or 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. Providing the FTC and state AGs with enforcement power backed up

with civil fining authority provides a far better approach for consumers, as evidenced by its success in policing violations of children's privacy through the Children's Online Privacy Protection Act.

Conclusion

Thank you again for the opportunity to testify today. The 21st Century Privacy Coalition looks forward to working with all Members of the Committee and all stakeholders to craft strong national privacy legislation. As Americans' online and offline activity involving personal information continues to grow in size and scope, consumers across the country deserve a clear understanding of how their personal information is being used and shared, and what is being done to protect their data from hackers and other bad actors.

The United States would benefit significantly from a unified, technology- and industry-neutral federal privacy law that applies uniformly to all entities, regardless of their business model. And new federal legislation that preempts other state and federal requirements would eliminate the consumer confusion and frustration, business uncertainty, and other debilitating effects such as reduced investment and innovation resulting from multiple and likely inconsistent regimes applying to the same information. Such a federal law would provide the greatest clarity and certainty about the rights of consumers and the responsibilities of companies that collect, use, or share consumers' personal information.

We encourage Congressional action that recognizes the yet-untapped potential of both the online world and the increasingly digitized offline world, while providing

Americans with the confidence that they will be safe when taking advantage of all these frontiers have to offer.