Testimony of

Jon Leibowitz

Co-Chair, 21st Century Privacy Coalition

on

Connecticut Raised Senate Bill 1108

Joint Committee on Government Administration and Elections

March 25, 2019

Chairmen Flexer and Fox, Vice Chairmen Haskell and Winkler, Ranking Members Sampson and France, and distinguished Members of the Joint Committee on Government Administration and Elections, thank you for the opportunity to testify at this important hearing. My name is Jon Leibowitz and I am a partner at the law firm of Davis Polk & Wardwell LLP. Along with Maureen Ohlhausen, I 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 across America that privacy legislation is necessary to bolster consumer confidence in 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, more importantly, because it is the right thing to do, members of the 21st Century Privacy Coalition enthusiastically support national privacy legislation that provides stronger and more meaningful privacy protections for American consumers. We are encouraged to see Connecticut's own Senator, Richard Blumenthal, leading a serious, bipartisan effort in the U.S. Senate Commerce Committee to pass a strong federal law that will affirm consumers' rights to control their personal data.

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

[1] The FTC has brought literally hundreds of privacy and data security cases, including well over 60 cases against companies for misusing or failing to reasonably protect consumer data, almost always with unanimous Commission votes.

personal information.[2] We support 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, and be held accountable for 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 laid out in the Commission's landmark 2012 Privacy Report.[3] We continue to adhere to such policies today.

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 against various companies by the FTC to ensure privacy and security of consumer information,

[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] *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.

as well as from the input of dozens of stakeholders (including businesses, privacy advocates, and academics), and multiple consumer privacy and data security workshops.

As Americans' online and offline activity involving personal data continues to grow in size and scope, consumers in Connecticut and across the country deserve a clear understanding of how their data is being used and shared as well as what is being done to protect data from hackers and other bad actors. The 21st Century Privacy Coalition appreciates your desire to ensure that the privacy rights of all Connecticut constituents are protected. And we applaud the technology- and industry-neutral approach—one that treats all data collectors the same—that the Committee seeks to implement in the bill before us.[4] To your credit, you understand 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 used.

However, additional state intervention in this quintessentially interstate issue is problematic, no matter how well-intentioned it may be. By its very nature, the Internet connects individuals across state (and national) lines. Put simply, data knows no state boundaries. A proliferation of differing state privacy rules would be infeasible to implement, and would create inconsistent privacy protections for consumers based on where they live, work, or happen to access online services. A Connecticut wireless customer visiting Texas should not have different privacy protections than a Texas wireless customer visiting Connecticut. Nor should a Connecticut resident enjoy different privacy protections when commuting to or at work in New York. This inconsistency could result in consumer confusion about the scope of their privacy

[4] Raised S.B. No. 1108, "An Act Concerning Consumer Privacy."

protections and the jurisdictions in which such protections apply. Indeed, you clearly recognize the problems of creating such a patchwork, as the privacy legislation before this Committee would preempt municipal and local regulations. The passage of such a measure could create barriers to the kind of investment and innovation that is a lifeblood of state economies.

In addition, multiple substantive aspects of this bill raise concerns not just for businesses seeking clarity on how to comply with its provisions, but also for consumers. As written, the bill includes a definition of "personal information" that is far too broad. The term would include information that "relates to," "describes," or "is capable of being associated with" an individual or household even if the individual is not identifiable. Tying the definition to "households" is also problematic. Not only is it likely that individuals living under the same roof will have different privacy preferences, but, when combined with the broad consumer rights offered, this definition may actually require businesses to reveal intimate personal information to an individual's relatives or roommates that the person had no desire to share with anyone. It could also force businesses to associate identifiable information with truly non-identifiable information in order to respond to access requests. Additionally, the bill's definition of "consumer" is so broad as to include employees, which raises issues far beyond the realm of privacy rights.

Like the California Consumer Privacy Act ("CCPA"), the bill also requires businesses to provide consumers with "specific pieces of personal information" that the business has collected about the consumer, suggesting that businesses could be required to provide even Social Security numbers or driver's license numbers to individuals

making access requests, greatly increasing the risk of fraud and harm to consumers. A better approach would be to limit the required disclosure to the types of information that the business has collected.

Moreover, the legislation sows doubt for businesses attempting to offer popular incentive programs to consumers that involve data collection, due to a nebulous requirement that the value of the benefit offered must be "directly related" to the value of the consumer's data to the consumer. Putting aside the imprecision of such a concept, the language disregards the importance of allowing consumers to make informed choices about the benefits they want to enjoy in the marketplace.

The data portability requirements in the bill also present operational challenges and are unclear. They would impose costs and burdens on businesses without providing any privacy benefit to consumers. We would note that the European General Data Protection Regulation ("GDPR") provides for data portability only with respect to the information that the consumer has provided to the business.

While we do believe federal legislation, rather than a state-by-state approach, should be enacted to ensure strong consumer privacy rights, we also believe it is critical to recognize that not only the FTC but also every State Attorney General should have a meaningful role to play in enforcing a national framework. State attorneys general around the country, including in Connecticut, have experience with requiring companies to honor their privacy commitments and maintain reasonable data security measures.[5]

[5] Connecticut in particular has been especially active in the privacy enforcement space. In 2010, the Connecticut Attorney General sued Health Net under the 2009 federal HITECH Act (regarding protected health information). In 2011, this state created one of the first special privacy units in the country before establishing the Privacy and Data Security Department within the State Attorney General's office in 2015. Connecticut was part of a 2013 multi-state investigation into allegations that Google circumvented default privacy settings to transmit advertising cookies. Connecticut also investigated Target for

For its part, the FTC has broad authority under Section 5 of the FTC Act to police the privacy and data security practices of marketplace participants, and it goes after companies when they break their privacy commitments to consumers or engage in unfair practices. The agency has held hundreds of companies, large and small, accountable when they violate the law, while remaining flexible enough to allow for innovation. The FTC has brought more than 500 cases to protect the privacy and security of consumer information, including those against Facebook, Google, and Dish Network. The Commission is also currently investigating Facebook to assess whether the company violated its 2011 consent agreement with the FTC.

We believe that the FTC and state attorneys general should have the authority to enforce a national privacy law, and that authority should include the ability to impose civil penalties on violators. But we also believe consumer privacy laws should not provide new private rights of action. These provisions often benefit attorneys while providing little relief to consumers, and divert company resources from compliance to litigation, ultimately not helping consumers who, at the end of the day, simply want companies to comply with the law. The broad private right of action in this bill is particularly concerning, because it applies to all of the provisions of the bill—not merely to security breaches, as in the CCPA. This could allow class action claims for inconsequential violations such as incorrect notice, which would burden courts and businesses without providing any useful deterrence, let alone remedies that actually benefit consumers. Providing the FTC and state attorneys general with enforcement

---

(continued….)

maintaining inadequate security protocols leading up to a massive data breach. These are just a few examples that demonstrate this state's dedication to protecting consumer privacy.

power backed up with civil fining authority provides a far better approach for consumers, as evidenced by its efficacy in policing violations of children's privacy through the Children's Online Privacy Protection Act ("COPPA").

Moreover, my own view is that the bipartisan effort currently working its way through the U.S. Senate Commerce Committee shows real promise for producing a strong, federal pro-consumer privacy law. We hope that this approach will be modeled on the 2012 FTC Privacy Report recommendations, including opt-in rights for sensitive information, opt-out rights for non-sensitive information, and inferred consent with regard to certain categories of operational uses of information by companies (such as in the case of order fulfillment, fraud prevention, and certain types of first-party marketing). We also hope that it will be technology- and industry-neutral, and provide enforcement authority with teeth for the FTC and state attorneys general so they can continue to fulfill their consumer protection mandate. I was proud of the recommendations my former agency made when we released the Privacy Report, and I continue to believe they form the pathway to the correct privacy regime for this country.

Why should you put your faith in the federal government getting something done? To be certain, that is a fair question. But the legislative dynamic is fundamentally different today than it was even a year or two ago. Forces are aligned for federal privacy legislation in a way we have not seen before. Beyond broadband providers like the ones represented in the 21st Century Privacy Coalition, there is now an industry-wide consensus around the need for such a law. We have heard a chorus of support from other companies for a meaningful nationwide privacy framework that gives more power to consumers. Legislators are also listening to consumers' concerns about the collection,

use, and sharing of their online information, and both Democrats and Republicans agree on the need to take action to bolster the privacy rights of our citizens.

In conclusion, while we understand and respect your eagerness to provide stronger privacy protections to the people of Connecticut, adding to a confusing patchwork of state rules is not the right way to achieve this goal. This is especially true for online privacy, which is an inherently interstate issue, and it should be enhanced by new federal legislation that includes greater enforcement authority for the FTC and state attorneys general. We respectfully ask that Connecticut defer consideration of Senate Bill 1108 while these important and promising federal efforts unfold. On behalf of the 21st Century Privacy Coalition, thank you again for your careful consideration of the issue.