STATEMENT OF JESSICA L. RICH

Of Counsel, Kelley Drye & Warren
Distinguished Fellow, Georgetown Institute for Technology Law and Policy

Before the

Senate Committee on Commerce, Science, and Transportation

On

ENHANCING DATA SECURITY

October 6, 2021

I. INTRODUCTION AND BACKGROUND

Chair Cantwell, Ranking Member Wicker, and members of this Committee, I am Jessica Rich, Of Counsel at Kelley Drye & Warren and a Distinguished Fellow at Georgetown University. I am pleased to be here today, testifying before this Committee on the need to strengthen data security protections in this country. I want to thank this Committee for its leadership and ongoing efforts on data privacy and security issues. I also want to make clear that my remarks today are my own, based largely on my years of experience in government service.

My background is as a lawyer and law enforcement official. I worked for over 26 years at the Federal Trade Commission (FTC), the last four as Director of its Bureau of Consumer Protection overseeing the agency's fraud, advertising, and privacy initiatives. Earlier in my FTC career, I launched the agency's very first privacy work, and then led and expanded these efforts for over a decade – bringing cases against companies that misrepresented their privacy practices and/or failed to secure consumer data, and developing rules to implement the Gramm Leach Bliley Act (GLB),[1] Children's Online Privacy Protection Act (COPPA),[2] and Fair and Accurate Credit Transaction Act.[3] In 2000, I led the FTC team that wrote the first of many reports to Congress[4] seeking stronger legal authority and remedies for data privacy and security – and I have testified, spoken publicly, and written many articles pleading the same case since.

[1] 15 U.S.C. § 6801 et seq.
[2] 15 U.S.C. § 6501 et seq.
[3] 15 U.S.C. § 1681 et seq.
[4] https://www.ftc.gov/sites/default/files/documents/reports/privacy-online-fair-information-practices-electronic-marketplace-federal-trade-commission-report/privacy2000.pdf.

Providing reasonable security for consumer data is at the heart of privacy protection. Even if a company determines not to sell or share its data with anyone, data can still be stolen through the proverbial "back door" if it is not protected from hackers or insiders with ill-intent.

And that is what we have seen, again and again over the years – scores of data breaches that harm consumers and businesses alike.[5] For consumers, data security failures can lead to fraud and identity theft, and the expense and worry of monitoring compromised accounts, changing passwords, and recovering losses.[6] For businesses, data security lapses can lead to loss of trust among customers, lost business, costly remedial efforts, and ransomware and other serious disruptions to operations.[7] Because commercial systems are highly connected to the nation's infrastructure, these compromises can undermine our national security as well.[8]

One of the problems is that current law fails to set clear and consistent standards for data security, or provide a solid basis for holding companies accountable. Indeed, most of the FTC's data security efforts are based on the FTC Act,[9] a law that was not designed for this purpose and is ill-suited for it in many ways. Among other things, the law does not establish clear standards for everyone to follow before problems occur – it is largely reactive. It does not cover non-profits, or companies engaged in common carrier activities. It does not authorize civil penalties for first time violations.

[5] See e.g., https://www.upguard.com/blog/biggest-data-breaches.
[6] See e.g., https://www.ftc.gov/system/files/documents/public_comments/2017/10/00004-141444.pdf.
[7] See e.g. https://www.fisglobal.com/en/insights/merchant-solutions-worldpay/article/how-the-consequences-of-a-data-breach-threaten-small-businesses.
[8] https://www.cisa.gov/critical-infrastructure-sector-partnerships.
[9] https://www.ftc.gov/sites/default/files/documents/statutes/federal-trade-commission-act/ftc_act_incorporatingus_safe_web_act.pdf.

And now, after the Supreme Court's ruling in the *AMG* case,[10] the law does not even allow the FTC to seek monetary relief in federal court under Section 13(b).

While the FTC has some authority over data security under certain sector-specific laws (Fair Credit Reporting Act,[11] GLB, and COPPA), these laws cover small slivers of the marketplace. Further, half of the states have now passed data security laws of their own, splintering the issue even further.[12]

The absence of federal standards in this area means that businesses lack clear rules to follow; consumers lack consistent and reliable protections, and remain confused and distrustful; and the FTC turns somersaults and faces legal challenges as it tries to fill the gaps. For all of these reasons, the U.S. urgently needs a federal standard that would bring stronger protections and greater clarity to the marketplace.

II. KEY QUESTIONS IN THE DATA SECURITY DEBATE

As this Committee is well aware, despite growing support for the *concept* of a federal data security law, many questions and disagreements remain about what it would include. So, to get right to the point, I offer my thoughts (below) on some key questions that always arise when the prospect of a federal data security law is discussed.

[10] https://www.supremecourt.gov/opinions/20pdf/19-508_l6gn.pdf.
[11] 15 U.S.C. § 1681 et seq.
[12] https://www.ncsl.org/research/telecommunications-and-information-technology/data-security-laws.aspx.

Should data security be addressed in a standalone federal law or as part of a federal privacy law? Including data security as part of a federal privacy law has the advantages of ensuring that privacy and data security requirements are harmonized; that consumers gain comprehensive protections all at once; and that companies can move forward with compliance plans on both fronts. Nevertheless, passing a data security law on its own would still advance data protection in this country considerably.

Who should enforce a federal data security law? The FTC, at the federal level. It has deep background and expertise in this area from over 20 years of enforcement experience and policy leadership; a strong commitment to the issue, and relationships with key sister agencies here and abroad (the Department of Justice, Health and Human Services, and international privacy enforcers and regulators, among others). With enhanced legal authority, the FTC could hit the ground running in a way no other agency could (and certainly not a brand new one). Providing the FTC with additional resources (the topic of last week's hearing) would also be critically important.

As discussed below, the State Attorneys General also should be fully empowered to enforce the federal law.

What elements should be included in such a law? The new law should fill many of the gaps discussed above:

First, it should extend across the marketplace to provide comprehensive protection to consumer and a level playing field to businesses. This means giving the FTC jurisdiction over non-profits and common carriers.

Second, the law should extend broadly to any data that, if not protected, could be used to cause consumer harm. In particular, the law should cover data that is reasonably *linkable* to a consumer, and should include categories of data that go well beyond account numbers – *e.g.*, account credentials, health data not covered by the Health Insurance Portability and Accountability Act,[13] and precise geolocation data.

Third, the law should provide clarity about companies' obligations while also giving them flexibility to tailor their data security protections to their business models. This means taking a process-based approach that includes certain key elements: (1) regular risk assessments (2) effective safeguards to limit the risks (3) a data security plan that is socialized throughout the company (4) training and oversight of employees and vendors (5) regular evaluation and updates to the plan and safeguards, and (6) accountability and oversight by expert personnel who report to the highest levels of the company. In addition, there should be requirements or incentives for companies to minimize unnecessary data collection and storage, as this is a huge source of risk to data.

[13] https://www.govinfo.gov/content/pkg/PLAW-104publ191/pdf/PLAW-104publ191.pdf.

Finally, of critical significance, the law should include the authority for the FTC (and the states) to obtain civil penalties and (in light of the *AMG* ruling) consumer redress – to deter misconduct and compensate consumers for their losses.[14]

Does a process-based approach provide sufficient guidance to companies as to their obligations? This question has been a source of debate. Companies have sometimes argued that they want more specific guidance, even as they also say they want flexibility. To address this concern, the federal law could direct the FTC to issue periodic guidance providing detailed, up-to-date information regarding security measures and technologies that companies should consider adopting. The guidance would not itself be enforceable, but it could provide valuable information that could be updated on a regular basis.

Does the FTC need rulemaking to implement a federal data security law? A key purpose of rulemaking is to ensure that a law keeps pace with rapid technological and market changes. Here, if the law takes a process-based approach and also directs the FTC to issue periodic guidance, full rulemaking authority may not be necessary. However, there may be specific issues for which rulemaking is needed – notably, what type of data should be covered under the law, an important issue that is likely to evolve over time.

Should the law preempt state laws in this area? Preemption has the advantage of ensuring clarity and consistency in an area that, as here, is already complex and costly. On the other hand, the states

[14] I did not include breach notification in these recommendations. With state breach notification laws now in effect in all 50 states, I believe including this issue would be highly disruptive to the goals of passing federal data security legislation.

have shown leadership in this area and their continued efforts could help strengthen protections and accountability nationwide. A good middle ground would be to preempt state data security laws while fully empowering the states to enforce the federal law. The law could provide a mechanism for coordination, similar to the coordination provisions in COPPA.

Should the law grant a private right of action? Ideally, a private right of action should not be necessary. One of the main arguments in support of a private right of action is that the FTC, with its limited resources, cannot possibly police the marketplace adequately to promote compliance, deter wrongdoers, and obtain recourse for injured consumers. A strong federal law could address these concerns by giving the FTC the legal tools and resource it needs, empowering the states to enforce the federal law, and including strong remedies for violations.

Federal and state enforcement – with no private right of action – would also facilitate more consistency, and prevent the types of class actions that have benefited lawyers more than consumers.

However, stakeholders have debated this issue for decades with no resolution. To bridge the divide, Congress could consider some middle-ground options – something Cam Kerry at Brookings[15] and others have written about. For example, a private right of action could be limited to willful and repeated violations and/or actual damages. It also could require proof of tangible harm, such as when data security failures result in fraud or identity theft; indeed, the recent Supreme Court decision in *Trans Union*,[16] which defined privacy injury fairly narrowly for purposes of standing

[15] https://www.lawfareblog.com/privacy-legislation-private-right-action-not-all-or-nothing-proposition.
[16] https://www.supremecourt.gov/opinions/20pdf/20-297_4g25.pdf.

in private actions, may already have compelled this outcome. Additionally, a private right of action could be subject to a right to cure, as in California's privacy law,[17] but that right would need to be clearly defined.

III. CONCLUSION

I would be happy to assist the Committee as it continues its work on this important issue. Thank you for allowing me to share my views today.

[17] https://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?division=3.&part=4.&lawCode=CIV&title=1.815.