STATEMENT OF JESSICA L. RICH

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

Before the

Subcommittee on Consumer Protection and Commerce
Committee on Energy and Commerce
United State House of Representatives

On

"HOLDING BIG TECH ACCOUNTABLE: LEGISLATION TO BUILD A SAFER INTERNET"

December 9, 2021

I. INTRODUCTION AND BACKGROUND

Chair Schakowsky, Ranking Member Bilirakis, and members of this Subcommittee, I am Jessica L. 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 holding big tech accountable and building a safer internet. I want to thank this Committee for its leadership and ongoing efforts on consumer protection, privacy, and related 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 the Bureau of Consumer Protection overseeing the agency's efforts to protect consumers from illegal marketing, advertising, and privacy practices. Earlier in my FTC career, I launched the agency's very first work to protect consumer privacy and data security, and then led and expanded these efforts for over a decade – bringing cases against numerous companies that failed to protect consumers' personal information, 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 privacy – and I have testified, spoken publicly, and written many articles pleading the same case since.

II. THE NEED FOR A COMPREHENSIVE FEDERAL PRIVACY LAW

The focus of my testimony today is on that very issue – privacy. For over two decades, Congress has debated whether to pass a comprehensive data privacy law. Scores of bills have come and gone with no action. Meanwhile, Europe and many other countries have moved ahead to enact detailed data protection regulations, and three states (California, Virginia, and Colorado) have done the

---

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 *Privacy Online: Fair Information Practices in the Electronic Marketplace: A Report to Congress* (FTC, May 2000), https://www.ftc.gov/sites/default/files/documents/reports/privacy-online-fair-information-practices-electronic-marketplace-federal-trade-commission-report/privacy2000.pdf.

same, adding to the cacophony of privacy laws that exists across jurisdictions, market sectors, and topic areas.

I understand that privacy is not the chief focus of this hearing. However, I am highlighting this issue in my testimony because the need for federal privacy legislation has never been greater; because many of the issues being considered at this hearing could be addressed, at least partially, in a privacy law; and because a privacy law would advance some of Congress' broader goals regarding the tech platforms and marketplace fairness.

Put simply (and borrowing from the title of this hearing), I believe that passing a federal privacy law is one of the most important things that Congress could do to "hold big tech companies accountable" and "build a safer internet." Further, given the progress made during the past two years on this issue – in both the House and the Senate – success should be within reach.

Here are some of the reasons why federal privacy legislation is needed now:

For Consumers

Survey upon survey shows that consumers are concerned and confused about their privacy and believe that they have little control about how companies collect, use, and share their personal information.[5] For good reason. In recent years, consumers have been the victims of massive and continuing data breaches,[6] data collection and abuses have exploded online,[7] and companies have increasingly made decisions about individuals using algorithms and profiles that predict consumers' behavior based on assumptions and stereotypes.[8]

---

[5] See *Americans and Privacy: Concerned, Confused, and Feeling Lack of Control Over Their Personal Information* (Pew Research Center, Nov. 2019), https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information/.

[6] See *The 60 Biggest Data Breaches* (Upguard, Dec. 2021), https://www.upguard.com/blog/biggest-data-breaches.

[7] See *Privacy International*, https://privacyinternational.org/examples.

[8] See *Algorithmic Bias Detection and Mitigation* (Brookings, May 2019), https://www.brookings.edu/research/algorithmic-bias-detection-and-mitigation-best-practices-and-policies-to-reduce-consumer-harms/.

Incredibly, as this Subcommittee knows, there is no law that protects consumer privacy nationwide. Instead, there are multiple laws that apply to certain sectors, jurisdictions, entities, and fact patterns.[9] If consumers want to decipher how companies collect and use their data, they need to read hundreds of lengthy privacy policies – often confusing, incomplete, and/or from companies they have never heard of. Further, without consistent rules governing consumer privacy, it is impossible to educate consumers about their rights, and thus enlist them in policing the marketplace, because their rights (or lack thereof) depend on the situation.

Consumers need a clear and consistent privacy law that they can rely on to protect them across jurisdictions and market sectors. Passing one would help build a safer internet.

For Businesses

Businesses are similarly confused about our privacy laws. Even as gaps in these laws leave consumers largely unprotected, they impose a huge compliance burden on companies trying to understand and follow them. At the federal level, we have the FTC Act, as well as numerous sector-specific laws – a veritable alphabet soup that includes COPPA, HIPAA, FCRA, GLBA, TCPA, FERPA, ECPA, CAN-SPAM, CPPA (the federal one), VPPA, GINA, and the CPNI rules. At the state level, there are the three state-wide laws mentioned above (with likely more to come), and yet again more sector-specific laws. For multinational companies, we have the General Data Protection Regulation (GDPR) and many other foreign laws and rules.

The lack of consistent standards allows the unscrupulous to exploit gaps and loopholes, disadvantaging honest companies. Further, the cost of navigating multiple laws and regulations benefits the tech platforms and other large companies that have the funds to afford it. So, too, does the emphasis in many existing laws on stopping third-party sharing (as opposed to stopping data abuses by everyone) because large companies have greater ability than small ones to keep their operations in-house.

[9] See *Data Protection: An Overview* (Congressional Research Service, March 2019), https://crsreports.congress.gov/product/pdf/R/R45631.

Businesses need a clear and consistent federal privacy law to help them navigate a difficult regulatory environment. Even if existing laws remain on the books, a federal law can create a more coherent framework for compliance. A federal law also could create a level playing field by imposing the same rules on everyone, and avoiding the pitfalls that have given advantages to the tech platforms and other large companies.

For Enforcers

The lack of clear privacy standards has undermined the FTC too – the nation's chief privacy enforcer at the federal level. Since the late 90s, most of the FTC's privacy efforts have been based on Section 5 of the FTC Act,[10] 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. And now, after the Supreme Court's ruling in the *AMG* case, the law does not even allow the FTC to seek monetary relief in federal court under Section 13(b).

Despite the shortcomings of the law, the FTC has brought hundreds of cases and obtained record-breaking settlements against companies that have misrepresented their data practices or used data in ways that impose significant harm.[11] Nevertheless, with adequate legal authority (and resources) conferred by a federal law, the FTC could be much more effective in investigating, studying, and putting a stop to harmful data practices. Empowering the State Attorneys General authority to enforce the law would enhance this effectiveness even further.

While some have suggested that the FTC simply write its own privacy rules using its Section 5 (Magnuson-Moss) rulemaking authority, such an effort is unlikely to succeed – or at least unlikely to produce the comprehensive and credible rules that are needed here. Magnuson-Moss rulemaking is an arduous process – requiring proof of deception or unfairness, as well as prevalence, for every

[10] 15 U.S.C. §§ 41-58.

[11] See FTC *Privacy and Security Cases and Proceedings*, https://www.ftc.gov/enforcement/cases-proceedings/terms/245%2B247%2B249%2B262.

mandate, and imposing hearings, paperwork, and other hurdles every step of the way.[12] Many rules, less complicated than privacy, have taken years to complete.[13] Further, after all of these years of debate, Congress needs to make the tough decisions to ensure acceptance (and not endless lawsuits) among the broad range of affected stakeholders.

In addition, while the Build Back Better bill would provide privacy resources that the FTC now lacks, clearer direction from Congress is needed to ensure that the FTC has sufficient authority and credibility to be the nation's lead privacy enforcer.

To Advance Related Goals Embraced by this Subcommittee and Many Others

The benefits discussed above would assist consumers and businesses, promote a level playing field in the marketplace, and strengthen the hands of the FTC and State AGs. Accomplishing these goals would be significant and historic for both data protection and competition in this country.

But there's more. In recent years, policymakers and the public have come to accept that the issues surrounding the use of personal data reach well beyond traditional notions of privacy – to issues like discrimination, algorithmic fairness, accountability, and whistleblower protections, some of the very issues being considered at this hearing. In addition, imposing data security requirements on commercial entities – a key feature in any privacy bill – is important to protecting our critical infrastructure, given its connections to commercial systems.[14] Finally, passing a federal privacy law would help strengthen the U.S.' position internationally – in negotiations about U.S.- EU data transfers and similar matters.[15]

---

[12] 15 U.S.C. § 57a.

[13] See Credit Practices Rule, 40 Fed. Reg. 16,347 (proposed Apr. 11, 1975); 49 Fed. Reg. 7740 (issued Mar. 1, 1984; codified at 16 CFR pt. 444); Sale of Used Motor Vehicles, 41 Fed. Reg. 1089 (proposed Jan. 6, 1976); 49 Fed. Reg. 45,692 (issued Nov. 19, 1984, codified at 16 CFR pt. 455).

[14] See *Critical Infrastructure Sector Partnerships*, https://www.cisa.gov/critical-infrastructure-sector-partnerships.

[15] See *U.S.-EU Privacy Shield and Transatlantic Flows* (Congressional Research Service, Sept. 2021), https://crsreports.congress.gov/product/pdf/R/R46917.

In short, this Subcommittee and Congress as a whole can achieve many important goals by enacting a federal privacy law – more than can be achieved by adding yet more sectoral requirements to the confusing mix of current laws now governing U.S. data and technology.

III. CONCLUSION

Thank you for inviting me here today. I stand ready to assist the Subcommittee and its members and staff with its ongoing work related to consumer protection and privacy.