STATEMENT OF JESSICA RICH

Of Counsel and Senior Policy Advisor for Consumer Protection
Kelley Drye & Warren LLP

Before the

Subcommittee on Innovation, Data, and Commerce
Committee on Energy and Commerce
United State House of Representatives

On

"PROMOTING U.S. INNOVATION AND INDIVIDUAL LIBERTY THROUGH A NATIONAL STANDARD FOR DATA PRIVACY"

March 1, 2023

I. INTRODUCTION AND BACKGROUND

Chair McMorris Rodgers, Ranking Member Pallone, Chairman Bilirakis, Ranking Member Schakowsky, and members of this Subcommittee, I am Jessica Rich, Of Counsel and Senior Policy Advisor for Consumer Protection at Kelley Drye & Warren, and a Distinguished Fellow at Georgetown University. I am pleased to be here today, testifying before this Subcommittee on setting a national standard for data privacy. I want to thank this Committee for its leadership and ongoing efforts on data privacy 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 harmful marketing, advertising, and data privacy and security practices. Much of my FTC career was devoted to data privacy and security. I was the first manager of the FTC's privacy program, starting in the late 1990s, and led its expansion as a division manager, and later as Deputy Director and then Director of the Bureau of Consumer Protection. In my various roles, I developed or oversaw enforcement against hundreds of companies that failed to protect consumers' personal information; rulemakings to implement privacy laws such as the Gramm-Leach-Bliley Act (GLBA),[1] the Children's Online Privacy Protection Act (COPPA),[2] and the Fair and Accurate Credit Transactions Act (FACTA);[3] and educational and policy initiatives to highlight emerging issues and promote best practices.

I also wrote or oversaw multiple recommendations to Congress seeking stronger legal authority and remedies for privacy, starting in 2000[4] and then echoed and refined in subsequent years.[5] I left the agency in 2017, but I have continued to press for a federal privacy law in Congressional

---

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* (May 2000) ("2000 Report"), https://www ftc.gov/sites/default/files/documents/reports/privacy-online-fair-information-practices-electronic-marketplace-federal-trade-commission-report/privacy2000.pdf.

5 See, e.g., *Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers* (March 2012), https://www.ftc.gov/reports/protecting-consumer-privacy-era-rapid-change-recommendations-businesses-policymakers.

testimony, op-eds, and speeches because of its importance to consumers, businesses, the FTC, and my longtime commitment to the issue.[6]

II. THE NEED FOR A COMPREHENSIVE FEDERAL PRIVACY LAW

I am here today to plead the same case yet again. The need for a federal privacy law has never been greater, and there is no substitute for Congressional action here. For over two decades, Congress has debated the issue. While Congress did pass some sector-specific legislation like COPPA and GLBA, it has repeatedly failed to act on comprehensive legislation. Meanwhile, Europe and countries all over the world moved ahead with detailed data protection laws, as have five U.S. states, with more in the pipeline.[7] All states now have data breach notification laws;[8] about half have data security laws;[9] and many also have sector-specific laws, like Illinois' Biometric Information Privacy Act.[10]

This "patchwork" (as it is so often called) is confusing and costly for consumers and businesses alike, and getting more so. Consumers need a strong and consistent law to protect them across jurisdictions and market sectors, and to clarify what privacy rights they should expect and demand as they navigate the marketplace. Businesses – especially small and medium sized ones – need to know what the rules are without having to spend millions of dollars on attorneys and overly complex compliance schemes. We have just the opposite now – a rolling wave of new and disparate privacy laws that confuse everyone and require an armada of experts to interpret.

Federal privacy legislation is the best way – and indeed the only way – to create a consistent set of rules that protect consumers nationwide. It will bring clarity for consumers and businesses; level the playing field between large and small companies; cast a wide net of protection that can

---

6 See, e.g., *Give the FTC Some Teeth to Guard our Privacy*, New York Times Op-Ed (August 2019), https://www.nytimes.com/2019/08/12/opinion/ftc-privacy-congress html.

7 See *IAPP State Privacy Legislation Tracker*, https://iapp.org/resources/article/us-state-privacy-legislation-tracker/.

8 See *Security Breach Notification Laws* (National Conference of State Legislatures or "NCSL"), https://www.ncsl.org/technology-and-communication/security-breach-notification-laws.

9 See *Data Security Laws – Private Sector* (NCSL), https://www ncsl.org/technology-and-communication/data-security-laws-private-sector.

10 740 ILCS 14.

address issues like discrimination and the misuse of kids' and teens' data; significantly boost enforcement and remedies for violations; and provide much-needed credibility abroad.

Although I could expand on each of the above points, my testimony today will focus on a related issue that is just as important – which is why *the FTC* needs a federal privacy law. As much as the FTC has been able to do with the tools that it has, it needs more authority from Congress to be a truly effective privacy enforcer. That's why the FTC has asked Congress so many times to pass federal privacy legislation. That's also likely why all three of the FTC's Democratic Commissioners, even as they launched their Section 18 (a/k/a "Mag-Moss") rulemaking on Commercial Surveillance and Data Security[11] (hereinafter "Privacy Rulemaking"), stated or implied that they would back away from the rulemaking if Congress were to pass a comprehensive privacy law.[12]

Indeed, under current law, the FTC's authority is limited, whether pursuing case-by-case enforcement or attempting a Mag-Moss rulemaking. Only Congress can establish the kind of broad-based protections contained in recent privacy bills such as the ADPPA. And only Congress can put to rest the issues that have been debated for years – notably whether to preempt state privacy laws and/or grant a private right of action, and how much discretion the FTC should have to shape the requirements (i.e., through rulemaking). Below, I provide more details about some of the strengths and limits of the FTC's privacy authority.

III. THE FTC'S PRIVACY AUTHORITY

1. Background on the FTC's privacy program

The FTC built its privacy program almost entirely around Section 5 of the FTC Act, a law that was written long before the arrival of the Internet.[13] That's because, in the mid-1990s, when the Internet

---

[11] See *Commercial Surveillance and Data Security Rulemaking*, https://www.ftc.gov/legal-library/browse/federal-register-notices/commercial-surveillance-data-security-rulemaking.

[12] Despite her support for stronger federal privacy mandates, Republican Commissioner Wilson dissented from the rulemaking, stating that Congressional action is the best course. All of the Commissioners' statements can be found at https://www ftc.gov/news-events/news/press-releases/2022/08/ftc-explores-rules-cracking-down-commercial-surveillance-lax-data-security-practices.

[13] 15 U.S.C. Sec. 45.

did arrive, there were very few U.S. laws (federal or state) that specifically addressed privacy. After holding hearings on what the Internet would mean for consumers and competition, the FTC quickly recognized that privacy would be a serious concern. It therefore sought to use Section 5, its general law prohibiting "unfair or deceptive" practices, to address this issue.[14]

Since then, the FTC has used Section 5 to challenge the data practices of a wide range of companies, including retailers, data brokers, mortgage companies, pharmacies, software companies, mobile apps, and most of the major tech companies.[15] The cases have spanned a wide range of fact patterns, too – false or misleading data privacy and security statements or settings,[16] including about children's data;[17] breaches of financial[18] and health information,[19] and even personal data about extramarital affairs;[20] spyware in people's homes;[21] and a wide range of other alleged violations.

The FTC has bolstered this enforcement, and increased its influence and visibility, with frequent use of the "bully pulpit" – including workshops and reports highlighting emerging issues and recommending best practices; consumer and business guidance; and testimony and

---

[14] See *2000 Report*, supra at n. 4, for discussion of the FTC's early privacy efforts.

[15] See *Privacy and Security Enforcement,* https://www.ftc.gov/news-events/topics/protecting-consumer-privacy-security/privacy-security-enforcement. There is a misperception that the FTC shied away from using unfairness until recently. In fact, many of the FTC's data privacy and security cases have been based on unfairness.

[16] See, e.g., *FTC Imposes $5 Billion Penalty and Sweeping New Privacy Restrictions on Facebook ("Facebook Settlement")*, https://www.ftc.gov/news-events/news/press-releases/2019/07/ftc-imposes-5-billion-penalty-sweeping-new-privacy-restrictions-facebook.

[17] See, e.g., *FTC Sues Failed Website, Toysmart.com, for Deceptively Offering for Sale Personal Information of Website Visitors*, https://www ftc.gov/news-events/news/press-releases/2000/07/ftc-sues-failed-website-toysmartcom-deceptively-offering-sale-personal-information-website-visitors.

[18] See, e.g., *Agency Announces Settlement of Separate Actions Against Retailer TJX, and Data Brokers Reed Elsevier and Seisint for Failing to Provide Adequate Security for Consumers Data,* https://www.ftc.gov/news-events/news/press-releases/2008/03/agency-announces-settlement-separate-actions-against-retailer-tjx-data-brokers-reed-elsevier-seisint.

[19] See, e.g., *Electronic Health Records Company Settles FTC Charges It Deceived Consumers About Privacy of Doctor Reviews*, https://www.ftc.gov/news-events/news/press-releases/2016/06/electronic-health-records-company-settles-ftc-charges-it-deceived-consumers-about-privacy-doctor.

[20] See, e.g., *Operators of AshleyMadison.com Settle FTC, State Charges Resulting From 2015 Data Breach that Exposed 36 Million Users' Profile Information*, https://www ftc.gov/news-events/news/press-releases/2016/12/operators-ashleymadisoncom-settle-ftc-state-charges-resulting-2015-data-breach-exposed-36-million.

[21] See, e.g., *FTC Halts Computer Spying*, https://www ftc.gov/news-events/news/press-releases/2012/09/ftc-halts-computer-spying.

recommendations to Congress.[22] Often, the FTC faced strong headwinds from industry and members of Congress, who opposed, not only the FTC's efforts, but any attempts to strengthen federal privacy laws.

Although Congress passed some sectoral privacy laws in the late 1990s and early 2000s (including COPPA, GLBA, and FACTA), the FTC Act continues to serve as the agency's core legal authority in privacy, given its broad scope relative to the sectoral laws. Most of the cases brought against the large tech companies, for example, were based on Section 5.[23]

Significantly, though, virtually all of the FTC's privacy and data security cases are settlements. That means that many of the legal theories advanced, as well as the remedies obtained, have never been tested in court.[24]

2. Limits of Section 5

The FTC's success in building a substantial and influential data privacy and security program can sometimes mask the limits of its legal authority in this area. In fact, Section 5 was not designed for privacy and is ill-suited for it in various ways. On the one hand, it has provided the FTC with substantial flexibility to tackle a wide array of practices. But on the other, the concepts of "deception" and "unfairness" contain many gaps and shortcomings when it comes to privacy. These shortcomings have become increasingly problematic as data use has proliferated and become more complex.

As a reminder, to prove deception, the FTC must show that there is a material representation, omission, or practice that is likely to mislead a reasonable consumer.[25] To prove unfairness, the FTC must show that a practice causes or is likely to cause substantial injury to consumers that

---

[22] See *FTC Policy Work on Privacy and Data Security*, https://www ftc.gov/news-events/topics/protecting-consumer-privacy-security/ftc-policy-work.

[23] See, e.g., *Facebook Settlement*, supra at n. 16; *Google Will Pay $22.5 Million to Settle FTC Charges it Misrepresented Privacy Assurances to Users of Apple's Safari Internet Browser*, https://www.ftc.gov/news-events/news/press-releases/2012/08/google-will-pay-225-million-settle-ftc-charges-it-misrepresented-privacy-assurances-users-apples.

[24] One notable exception is the *Wyndham* case, in which the 3rd Circuit upheld the FTC's authority to challenge lax data security practices as unfair. *FTC v. Wyndham Worldwide Corp.*, 799 F. 3d 240 (2015).

[25] *Policy Statement on Deception*, https://www.ftc.gov/legal-library/browse/ftc-policy-statement-deception.

cannot reasonably be avoided by consumers, and is not outweighed by countervailing benefits to consumers or competition.[26]

One challenge is that Section 5 (and associated case law) was developed with traditional commercial transactions in mind – such as when a company sells, and a consumer purchases, a product or service (such as a sweater, tractor part, or investment) for a particular purpose and the consumer does not receive the goods or services intended or expected. In such situations, privacy may not be top-of-mind for consumers as they consider the transaction, even if they care about it in a general sense. In the case of the sweater, consumers may be thinking about its appearance, fit, or fabric, not whether the company stores credit card numbers securely, or sells consumer data to third parties. This can make it difficult to show that privacy was *material* to a consumer's decision to purchase the product or service.

Another challenge is that proving a practice "causes or is likely to cause" substantial injury for purposes of unfairness has always been a conundrum in privacy, especially since the concept of privacy injury can be so subjective. Is emotional or reputational injury sufficient? Is the mere release of data (even sensitive data) enough? How sensitive must data be to have its sale or compromise rise to the level of "likely" substantial injury? The FTC's Unfairness Statement (which courts still cite in their opinions) says that "emotional impact" and other "subjective" types of harm will not ordinarily make a practice unfair, but might do so in "extreme cases" when "tangible injury" can be shown.[27] Similarly, the Supreme Court has held that "concrete harm," and not the "mere risk of future harm," is necessary to confer standing to plaintiffs in privacy class actions.[28] The FTC must continuously navigate the issue of harm when it comes to privacy.

Yet another problem is that Section 5 does not establish clear standards for companies to follow before problems occur – it is almost wholly reactive. It does not tell businesses, for example, what privacy disclosures and choices they need to provide to consumers, or what data uses are so

---

[26] 15 U.S.C. § 45(n). The statutory test, enacted by Congress in 1994, superseded the FTC's Policy Statement on Unfairness ("Unfairness Statement"), https://www.ftc.gov/legal-library/browse/ftc-policy-statement-unfairness. However, the FTC and the courts still refer to portions of the Policy Statement, especially its discussion of consumer harm, and many of its principles are baked into FTC case law.

[27] See *Unfairness Statement*, supra at n. 26.

[28] *TransUnion LLC v. Ramirez*, 141 S. Ct. 2190 (2021).

inherently risky or harmful that they should be avoided or modified. Instead, it allows the FTC to evaluate a company's practices after the fact, to determine whether they meet the unfairness and/or deception tests. (The FTC is trying to fix this problem by promulgating its Privacy Rule, but that faces obstacles of its own, as discussed below.)

In addition, certain requirements that appear in existing privacy laws and bills are an especially poor fit for Section 5. Is the failure to provide access or deletion rights to consumers, without more, deceptive or unfair? What about a company's failure, without more, to audit its practices using certain criteria, or to have its executives attest to the audit? Certainly, companies have agreed to these types of requirements in settlements (as so-called "fencing-in" to prevent the companies from committing additional violations in the future) but that doesn't mean that failure to take these steps meets the deception and/or unfairness tests, or that a court would make that determination.

Finally, the FTC Act does not cover non-profits or companies engaged in common carrier activities – limitations that have long created an obstacle to even-handed FTC enforcement. Nor does it authorize civil penalties for first time violations or, since *AMG*, allow the FTC to seek consumer redress in federal court under Section 13(b).[29] (A rulemaking would lay the groundwork for monetary relief, but cannot alter the FTC's jurisdictional limits.)

3. Magnuson-Moss rulemaking

The FTC is well aware of the limits discussed above. That's why it has repeatedly, on a bipartisan basis, asked Congress to pass a federal privacy law that includes specific privacy mandates; authority to obtain civil penalties; and jurisdiction over nonprofits and common carriers.[30]

Congress has not acted, which is frustrating for many. So after two decades of asking, the FTC has moved ahead on its own, by launching its Privacy Rulemaking under Mag-Moss.

---

[29] Given the difficulty of quantifying many types of privacy injuries, penalties are often the better remedy.

[30] See, e.g., *FTC Report to Congress on Privacy and Security* (September 2021), https://www.ftc.gov/system/files/documents/reports/ftc-report-congress-privacy-security/report_to_congress_on_privacy_and_data_security_2021.pdf; *Prepared Remarks of Chairman Joseph J. Simons on "Oversight of the Federal Trade Commission: Strengthening Protections for American's Privacy and Data Security,"* https://www.ftc.gov/legal-library/browse/prepared-remarks-chairman-joseph-j-simons-oversight-federal-trade-commission-strengthening.

The Mag-Moss process is more cumbersome than "normal" rulemaking under the Administrative Procedures Act (APA). That's because Congress deliberately added provisions to make it so, due to perceived overreach by the FTC in the 1970s (especially its proposal to ban TV food advertising to kids – known as "kid vid").[31] Of particular note, Mag-Moss requires the FTC to prove that each practice it seeks to regulate is unfair or deceptive, as well as prevalent. In other words, the FTC is confined to the very same legal standards that, as discussed above, create obstacles for privacy – and must prove prevalence, too.

Mag-Moss also includes an extra round of public comments, public hearings as requested by stakeholders, and a more rigorous standard for judicial review.[32] According to a professor who analyzed FTC rules developed under Mag-Moss, the average time it took to complete them was almost six years, versus less than a year for APA rules.[33]

In addition, a sometimes-forgotten Mag-Moss provision limits the FTC's authority to develop rules regarding kids' advertising. This provision, now found in Section 18(h) of the FTC Act, prohibits the FTC from promulgating "any rule in the children's advertising proceeding pending on May 28, 1980" (i.e., 'kid vid") or in any "substantially similar proceeding" based on unfairness.[34]

In July 2021, an FTC majority voted to simplify the Mag-Moss rulemaking procedures, to the extent that it could, by stripping away some steps that the FTC had previously added to the process through its own internal rules.[35] However, most of the cumbersome requirements appear in the law, which the FTC cannot change. In addition, the Commission appears to be charting an ambitious path forward in the Privacy Rulemaking, one that portends a very long process. In its first request for comment (the Advance Notice of Proposed Rulemaking, or ANPRM), the FTC

---

31 See, e.g., *The FTC as National Nanny* (Washington Post Editorial, March 1, 1978, at A22).

32 15 U.S.C. § 57a.

33 Jeffrey Lubbers, *It's Time to Remove the 'Mossified' Procedures for FTC Rulemaking* (G.W. Law Review, February 2015), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2560557.

34 15 U.S.C. § 57a(h).

35 *FTC Votes to Update Rulemaking Procedures, Sets Stage for Stronger Deterrence of Corporate Misconduct,* https://www.ftc.gov/news-events/news/press-releases/2021/07/ftc-votes-update-rulemaking-procedures-sets-stage-stronger-deterrence-corporate-misconduct. Among other things, the changes eliminated the need for a staff report analyzing the rulemaking record, and gave the Chair more authority to control the public hearings process.

discussed dozens of privacy topics, posed 95 questions, and touched on many controversial issues. Not surprisingly, the agency received over 11,000 comments from the public.

The obstacles here are enormous. To develop a rule of the breadth that Congress considered in the bipartisan ADPPA, the FTC would need to prove that many dozens of practices are both prevalent and unfair or deceptive, with all of the associated challenges discussed above. It must review and analyze thousands of comments (twice) and hold public hearings with numerous stakeholders clamoring to be heard. Even if the FTC is able to complete the rulemaking, litigation seems likely, whether based on the particular issues regulated or bigger picture questions about the FTC's legal authority here.[36]

Additionally, the FTC cannot resolve (or should not be the one to resolve) the most controversial issues in the privacy debate – whether to preempt state laws,[37] grant a private right of action, and/or impose limits on its own rulemaking discretion. Nor can it address the data practices of common carriers and non-profits – those entities would not be covered by an FTC rule.

IV. CONCLUSION

There is simply no substitute for federal privacy legislation. No other U.S. privacy regime or proposal can create the broad protections and consistent standards that the U.S. sorely needs. Congress must finally pass a federal privacy law to protect and reassure the American public.

[36] Multiple comments on the FTC's ANPRM argue that the FTC's proposal raise concerns under the "Major Questions" doctrine recently discussed by the Supreme Court in *West Virginia v. EPA*, 142 S. Ct. 2587 (2022).

[37] In theory, the FTC could try to preempt state privacy laws, or set its Privacy Rule as floor that the state laws could exceed (as it has proposed to do in its rulemaking to ban non-compete clauses). See e.g., *Fidelity Savings & Loan Assn. v. De La Questa,* 458 U.S. 141 (1982). However, any such proposal would likely draw legal challenge.