PREPARED TESTIMONY AND STATEMENT FOR THE RECORD
OF

WOODROW HARTZOG
ASSOCIATE PROFESSOR OF LAW
SAMFORD UNIVERSITY'S CUMBERLAND SCHOOL OF LAW

HEARING ON

"THE FEDERAL TRADE COMMISSION AND ITS SECTION 5 AUTHORITY: PROSECUTOR, JUDGE, AND JURY"

BEFORE THE

COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM
U.S. HOUSE OF REPRESENTATIVES

July 24, 2014
2154 Rayburn House Office Building
Washington, DC

I. INTRODUCTION

Chairman Issa, Ranking Member Cummings, and Members of the Committee, thank you for inviting me to appear before you and provide testimony. My name is Woodrow Hartzog and I am an associate professor of law at Samford University's Cumberland School of Law and an affiliate scholar at the Center for Internet and Society at Stanford Law School. I write extensively about information privacy law issues and have published well over a dozen law review articles and other scholarly works. Most relevant to this hearing, I, along with my co-author Professor Daniel J. Solove, have spent the last two years researching the Federal Trade Commission's regulation of privacy and data security issues, which I will collectively refer to as "data protection." In a series of articles, we have analyzed all 170+ FTC data protection complaints to find trends and understand the FTC's data protection jurisprudence.[1] My comments today will address what I've learned from this research.

I will focus my remarks on the FTC's work on data security and consumer privacy, and especially the scope of the FTC's authority to regulate data protection under Section 5 of the FTC Act. I will not address the specifics of any particular privacy or data security dispute. These comments are made in my personal, academic capacity. I am not serving as an advocate for any particular organization. My remarks will focus on two points.

First, I will discuss why the FTC's regulation of privacy and data security under Section 5 has served a critical function for the US system of data protection. Far from being an overall burden to industry, the FTC's involvement in data protection has given the heavily self-regulatory system of data protection necessary legitimacy and heft. Diminished FTC data protection authority would threaten the existence the U.S.-E.U. Safe Harbor which governs the international exchange of personal information. No other regulator has the same ability to enforce necessary yet quickly evolving protections like data security.

Second, I will discuss the scope and administration of the FTC's Section 5 authority. I have spent a considerable amount of time analyzing the entire body of FTC activity on data protection. Overall, the overwhelming pattern is that the FTC has acted conservatively, judiciously, and consistently. Given the ever increasing volume of data and accompanying risk of the information age, the role of the FTC in data protection seems both important and a natural consequence of the agency's charge to protect consumers.

---

[1] Daniel J. Solove & Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, 114 COLUM. L. REV. 583 (2014), available at http://ssrn.com/abstract=2312913; Woodrow Hartzog & Daniel J. Solove, *The Scope and Potential of FTC Data Protection*, 83 GEO. WASH. L. REV. (forthcoming 2015), available at http://ssrn.com/abstract=2461096; Daniel J. Solove & Woodrow Hartzog, *The FTC and Privacy and Security Duties for the Cloud*, 13 BNA PRIVACY & SECURITY LAW REPORT 577 (2014), available at http://ssrn.com/abstract=2424998; Woodrow Hartzog & Daniel J. Solove, *The FTC as Data Security Regulator: FTC v. Wyndham and its Implications*, 13 BNA PRIVACY & SECURITY LAW REPORT 621 (2014), http://docs.law.gwu.edu/facweb/dsolove/files/BNA%20FTC%20v%20Wyndham%20FINAL.pdf.

II. SECTION 5 IS THE LYNCHPIN OF U.S. DATA PROTECTION LAW

The most important grant of authority to the FTC in protecting consumers' personal information comes from Section 5 of the Federal Trade Commission Act. Under this statute, "unfair or deceptive acts or practices in or affecting commerce, are hereby declared unlawful."[2] The FTC first began to regulate data protection online in the 1990s by focusing on promises companies voluntarily made in their privacy policies. When companies later failed to live up to these promises, the FTC claimed that this was a deceptive trade practice.

In this way, the FTC used the predominantly self-regulatory approach to privacy and data security as its foundation to build a foothold in the area of data protection. Over time, the FTC expanded beyond enforcing privacy policies to a broader conception of deception, one that did not rely only on explicit promises made. The FTC also began to exercise its power to police unfair trade practices.

Today, the FTC has evolved into the most important data protection agency in the United States. The FTC plays two critical roles within the U.S. data protection ecosystem. It fills significant gaps left by the patchwork of statutes, torts, and contracts that make up the U.S. data protection scheme. The FTC also stabilizes the volatile and rapidly evolving area of data protection and provides legitimacy for the largely sectoral U.S. approach to data protection.

A. Filling Critical Gaps

In the current U.S. privacy regulatory system, the FTC has grown into the key lynchpin giving coherence to a partly self-regulatory system supported by a loose patchwork of data protection laws at the federal and state level. Unlike many other countries, in the U.S. there are a multitude of different laws regulating different industries rather than just one general law to regulate all collection and use of personal data.

Particular sectoral laws often leave gaps where entire industries lack privacy regulation. For example, there is no federal law that explicitly mandates data security for all online commerce. Without the FTC, some collections and uses of data would be unregulated. Through Section 5, the FTC sets a floor for commercial activity that otherwise cannot be practically regulated by consumers through contract, tort, or reputation.

Concerned about consumer concerns and trust, in the late 1990s online companies began voluntarily making promises about data protection in privacy policies. Initially, the FTC began enforcing these promises made in privacy policies, giving the promises a stronger backbone. The FTC's broad range of coverage spanned countless industries, thus plastering over the large gaps and crevices left in between sectoral laws. The FTC also brought a thin layer of coherence to the whole system, and this coherence has gradually thickened over the years.

[2] 15 U.S.C. § 45(a)(1).

The FTC currently remains a key lynchpin in the U.S. data protection regulatory regime. Self-regulation still plays a big role, with industry serving as the primary generator of best practice norms. Far from being externally imposed, the norms that the FTC has enforced have been developed by industry as well as consumer expectations. Instead of imposing top-down rules all at once, the FTC has integrated itself into a largely self-regulatory approach and gradually developed it into a more robust regulatory system.

B. The Stabilizing Function of the FTC

The FTC also stabilizes and legitimizes the U.S. approach to data protection. For example, the FTC plays a pivotal role in international confidence regarding privacy in the United States. The FTC is an essential component of the Safe Harbor Arrangement, which allows personal data to flow between the United States and European Union.[3] Without the FTC's data protection enforcement authority, the E.U. Safe Harbor agreement and other arrangements that govern the international exchange of personal information would be in jeopardy.

With so many different sources of law and regulation in the United States, the FTC can also play a harmonizing role. The broad scope of Section 5, which allows the FTC to respond to many different kinds of threats to data protection, can obviate the need for new laws. Section 5 ensures fewer gaps and fewer needs of states to protect their citizens in possibly very conflicting and burdensome ways. The FTC's power is broad enough to develop over time a more coherent and comprehensive body of regulatory activity.

III. THE SCOPE AND ADMINISTRATION OF THE FTC'S AUTHORITY UNDER SECTION 5

The FTC's most important tool for protecting the data of consumers is its grant of authority to regulate unfair and deceptive trade practices under Section 5. Congress granted the FTC the authority to interpret the nature of deceptive practices, which the agency summarized in a 1983 policy statement: A deceptive trade practice is a "misrepresentation, omission or other practice, that misleads the consumer acting reasonably in the circumstances, to the consumer's detriment."[4] Unfair trade practices are defined by statute as a practice that "causes or is likely to cause substantial injury to consumers which is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition."[5] This broad

[3] See, e.g., Commission Decision 2000/520/EC, 2000 O.J. (L 215) 7, 26–30 (discussing FTC enforcement authority); Issuance of Safe Harbor Principles and Transmission to European Commission, 65 Fed. Reg. 45,666 (July 24, 2000) (same); Int'l Trade Admin., U.S. Dep't of Commerce, U.S.-EU Safe Harbor Overview, Export.gov, http://www.export.gov/safeharbor/eu/eg_main_018476.asp (("Under the Federal Trade Commission Act, for example, an organization's failure to abide by commitments to implement the Safe Harbor Privacy Principles might be considered deceptive and actionable by the Federal Trade Commission.").

[4] Letter from James C. Miller III, Chairman, FTC, to Hon. John D. Dingell, Chairman, House Comm. on Energy & Commerce (Oct. 14, 1983) , reprinted in In re Cliffdale Assocs., Inc., 103 F.T.C. 110 app. at 175–84 (1984) (decision & order).

[5] 15 U.S.C. § 45(n) (2012).

grant of authority was designed precisely to avoid restrictive categories of practices which are unfair or deceptive.[6]

A. The Intentionally Broad Scope of Section 5

Other than the limitations inherent in the conceptualizations above, Congress has been explicit in eschewing hard boundary lines for what constitutes unfair and deceptive trade practices.

The scope of the FTC's deceptiveness jurisdiction has included broken promises of privacy and data security, deceptive actions to induce the disclosure of information, and failure to give sufficient notice of privacy invasive practices. Although the requirement that a deception be material to consumers constrains the scope of FTC enforcement power, misrepresentations can be made in virtually any context, including boilerplate policies, marketing materials, and even the design of websites.

The FTC's unfairness authority is also comprehensive. According to the FTC, "The present understanding of the unfairness standard is the result of an evolutionary process. The statute was deliberately framed in general terms since Congress recognized the impossibility of drafting a complete list of unfair trade practices that would not quickly become outdated or leave loopholes for easy evasion."[7]

B. A Conservative, Judicious, and Consistent Approach

A review of every FTC complaint related to data protection reveals that the agency has acted in a conservative way. The FTC's data security program began under the direction of then-Chairman Timothy Muris and has continued, without any major course change, under the stewardship of Chairwoman Deborah Majoras, Chairman William Kovacic, Chairman Leibowitz, and now Chairwoman Ramirez.

The FTC actually brings a relatively very small number of data security complaints. Compared to the number of total reported data breaches, the likelihood that a company will be subject to a FTC enforcement action is quite low. The Privacy Rights Clearinghouse has reported that since 2005 there have been over 4300 data breaches made public with a total of over 868 million records breached.[8] Yet the FTC has filed only 55 total data security-related complaints, averaging around five complaints a year since 2008.[9]

---

[6] *See* H.R. Conf. Rep. No. 1142, 63d Cong., 2d Sess., at 19 (1914) (finding that, regarding unfairness, if Congress "were to adopt the method of definition, it would undertake an endless task").

[7] FTC Policy Statement on Unfairness, Appended to International Harvester Co., 104 F.T.C. 949, 1070 (1984). *See* 15 U.S.C. § 45(n). *See also* CHRIS HOOFNAGLE, FEDERAL TRADE COMMISSION PRIVACY LAW AND POLICY (forthcoming 2015).

[8] PRIVACY RIGHTS CLEARINGHOUSE, *Chronology of Data Breaches: Security Breaches 2005 – Present*, https://www.privacyrights.org/data-breach.

[9] FEDERAL TRADE COMMISSION, *Legal Resources: Privacy and Security*, http://www.business.ftc.gov/legal-resources/29/35.

Instead, the FTC typically pursues only what it considers to be egregious data security practices. Each data security complaint includes a litany of alleged security failures, including failures to identify assess and risk, failures to minimize the storage of data, and failures to implement reasonable administrative, technical, and physical safeguards. The FTC has remained notably consistent as it gradually develops its data security jurisprudence in incremental steps.

C. The Wide Consensus of Reasonableness-based Data Security Requirements

The FTC generally prohibits unreasonable data security practices "in light of the sensitivity and volume of consumer information it holds, the size and complexity of its business, and the cost of available tools to improve security and reduce vulnerabilities."[10]

What constitutes reasonable data security is determined virtually entirely by industry standard practices. This deference to industry keeps the FTC from promulgating data security rules in an arbitrary and inconsistent way. The FTC does not pull rules out of thin air. Rather, it builds upon the formidable and evolving body of knowledge in the data security field as well as the commonly implemented data security practices of companies to determine when custodians of personal information are engaging in unfair and deceptive data security practices.

A reasonableness standard is already one the most established and proven touchstones for regulating data security. Almost ten states require reasonable data security practices, rather than a specific list of prohibited or mandatory actions.[11] Congress has also explicitly embraced a reasonableness approach to data security. The Fair Credit Reporting Act (FCRA),[12] the Health Insurance Portability and Accountability Act (HIPAA),[13] and the Gramm-Leach-Bliley Act (GLBA)[14] all use reasonableness as a touchstone for determining the adequacy of data security measures.

Unfortunately, it is not possible to provide a "one size fits all" detailed checklist of reasonable data security practices. A determination of reasonable data security is far too dependent upon context. Yet a comparison of data security regulatory regimes that use a reasonableness standard shows that there are four central components of a reasonable approach to data security:

1) Identification of assets and risk
2) Data minimization
3) Administrative, technical and physical safeguards
4) Data breach response plans

---

[10] FEDERAL TRADE COMMISSION, *Commission Statement Marking the FTC's 50th Data Security Settlement* (January 31, 2014) http://www.ftc.gov/system/files/documents/cases/140131gmrstatement.pdf.
[11] *See* Woodrow Hartzog & Daniel J. Solove, *The Scope and Potential of FTC Data Protection*, 83 GEO. WASH. L. REV. (forthcoming 2015) at fns 80-83, available at http://ssrn.com/abstract=2461096.
[12] 16 C.F.R. § 682.3(a).
[13] 45 C.F.R. §§ 164.308-.314.
[14] 16 C.F.R. §§ 314.3-314.4.

Various frameworks exist to provide further detail for those operating in certain contexts, such as the framework and standards offered by the National Institute of Standards and Technology (NIST)[15] and the Payment Card Industry (PCI) Security Standards Council.[16]

Additionally, ample resources exist for companies looking for guidance on reasonable data security practices, many of which are free and easily accessed online. The Federal Trade Commission actively updates its resources on data security.[17] Scholarly articles, trade publications, and other sources of information are also readily available.[18]

A robust support system exists for companies seeking to provide reasonable data protection for consumers. There is a vast network of privacy professionals dedicated to helping companies understand their obligations under certain privacy regimes like the FTC. Technologists and other consultants can help companies of all sizes. These counselors have a nuanced understanding of data protection and the significance of the FTC complaints and are able to rely on the FTC's guidance as well as industry standards to competently advise their clients.

IV. CONCLUSION

Section 5 of the FTC Act has empowered the Federal Trade Commission to serve a central role in protecting consumer information. Just as importantly, the FTC's data protection jurisprudence helps create and sustain consumer trust in companies that collect and store consumers' personal information. It is very difficult for consumers to determine whether a company collecting their personal information has reasonable data security practices. This opacity decreases the incentive for companies to spend the resources necessary to establish reasonable data protection. The FTC's regulation of data protection under Section 5 allows consumers to transact with companies with greater confidence that their personal information will be safe and properly used.

Of course, as with any agency, there is always room for improvement of FTC enforcement. More detailed complaints and closing letters from investigations that do not result in a complaint are quite helpful to other companies and, to the extent that they are productive and feasible, should be encouraged. But the agency's power should be expanded rather than contracted. Diminishing FTC power will not ultimately make the climate easier for business. In fact, given the vital importance of data protection in commerce, a reduction in FTC authority would likely result in the passage of more

---

[15] NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, *Framework for Improving Critical Infrastructure Cybersecurity*, http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf.

[16] PCI SSC Data Security Standards Overview, https://www.pcisecuritystandards.org/security_standards/.

[17] FEDERAL TRADE COMMISSION, *Legal Resources: Privacy and Security*, http://www.business.ftc.gov/legal-resources/8/35.

[18] *See, e.g.* Joel Reidenberg, N. Cameron Russell, Alexander Callen, and Sophia Qasir, *Privacy Enforcement Actions*, CENTER ON LAW AND INFORMATION POLICY (June 2014), http://law.fordham.edu/assets/CLIP/CLIP_Privacy_Case_Report_-_FINAL.pdf; Travis D. Breaux & David Baumer, *Legally "Reasonable" Security Requirements: A 10-year FTC Retrospective*, 30 COMP. & SECURITY 178 (2011), http://www.cs.cmu.edu/~./breaux/publications/tdbreaux-cose10.pdf.

restrictive and conflicting state laws, more actions by state attorneys general, more lawsuits from private litigants, and more clashes with the E.U. concerning the overall strength of U.S. privacy law. In the long run, a weakened FTC would likely result in a more complicated and less industry-friendly regulatory environment.

Data protection is a complex and dynamic area. Section 5 enables the FTC to be adaptive and serve as a stabilizing force for consumers and companies.