MERCATUS CENTER
George Mason University

TESTIMONY

THE IMPORTANCE OF AVOIDING UNINTENDED CONSEQUENCES WHEN DEFINING HARM FOR DATA SECURITY AND DATA PRIVACY

Jennifer Huddleston
Research Fellow, Mercatus Center at George Mason University

House Committee on Oversight and Reform, Subcommittee on Economic and Consumer Policy

March 26, 2019

Good afternoon, Chairman Krishnamoorthi, Ranking Member Cloud, and distinguished members of the Subcommittee on Economic and Consumer Policy.

My name is Jennifer Huddleston and I am a research fellow at the Mercatus Center at George Mason University. My research focuses primarily on the intersection of law and technology as well as issues surrounding data security and data privacy. Thank you for the opportunity to discuss some of the important issues surrounding data security and the role and ability of agencies to protect consumer information. This is an important policy conversation in light of the historic Equifax breach that occurred in 2017 as well as continuing conversations around data breaches and data privacy, and it is important that Americans consider the possible unintended consequences in such policy.

Today I would like to focus on the following three points:

1. Regulators should avoid an expansive theory of harm in their approach to data security.
2. The Federal Trade Commission (FTC) has been the main agency for enforcing data security and data privacy, and its flexible approach has allowed innovation to flourish while still redressing consumer harm.
3. Policy solutions should be narrowly tailored and should focus on the unique position of credit reporting agencies.

THE PROBLEMS OF AN OVERLY EXPANSIVE DEFINITION OF HARM

Breaches of personal information have led to financial, emotional, and even physical harm, but as a 2018 FTC workshop report notes, there is not agreement regarding whether and when the government should intervene when a breach has occurred.[1] Too often it is easy to rush to intervention as a result of worst-case-scenario thinking in the light of a scandal and promote a seemingly definitive solution that could actually create more unintended consequences than the problems that it solves.[2] So far, the United States has avoided such an approach to data security, but when emotions and tensions run high in light of scandals such as the Equifax breach, America risks a response that leads to serious consequences later.

[1] *FTC Informational Injury Workshop: BE and BCP Staff Perspective* (Washington, DC: Federal Trade Commission, October 2018).
[2] Adam Thierer, "The Pursuit of Privacy in a World Where Information Control Is Failing," *Harvard Journal of Law & Public Policy* 36, no. 2 (2013): 409–54.

For more information or to meet with the scholar, contact
Mercatus Outreach, 703-993-4930, mercatusoutreach@mercatus.gmu.edu
Mercatus Center at George Mason University, 3434 Washington Blvd., 4th Floor, Arlington, Virginia 22201

An overly broad definition of information harm applied beyond carefully tailored requirements for specific narrow sectors as a result of headline-making data breaches could damage the information economy and America's innovation leadership. In contrast to the United States, the European Union has taken such an approach to data protection much to the detriment of innovation, competition, and growth in technology.[3] Such regulations can lead to innovators believing that it is simply too risky to pursue new solutions that may run afoul of regulators and entrenched firms.[4]

An overly broad definition may also not reflect the realities of data usage and collection and the benefits consumers often receive. As Geoffrey Manne stated at the FTC workshop on informational injury, "If risk of injury were enough to constitute injury, literally everything, literally the existence of these businesses, would increase the risk of injury and therefore be actionable."[5] Depending on the definitions of data and businesses, it is easy for a broad approach to include not just traditional data brokers, internet giants, or credit bureaus, but also main-street small businesses that happen to have customer information through loyalty programs or online presences.[6]

Not only can a broad definition of harm associated with the breach of personal information deter innovation, it can also be nearly impossible to enforce. As I noted in comments to the FTC on the issue of informational injury with my colleagues Chris Koopman, Adam Thierer, and Andrea O'Sullivan, "Opinions on what constitutes an adequate level of privacy are almost as varied as the personalities of the people who hold them, and these opinions evolve over time."[7] A static system based on the current options and fear is unlikely to solve the problems it intends in the same way that a flexible system could allow private parties to find or create the solutions that best fit their needs.

THE FTC'S ROLE IN DATA SECURITY AND DATA PRIVACY

The United States currently lacks an agency directly tasked with the regulation of data security or data privacy. While various agencies have provided guidance on the proper handling of data in their covered sectors, the FTC has become the agency that handles such issues more generally.

In the past 17 years, the agency has brought 65 cases involving consumers' personal data generally and more than 100 cases involving financial privacy and credit reporting under the Fair Credit Reporting Act and the Gramm-Leach-Billey Act.[8] This current approach stems largely from the FTC's Section 5 authority to protect consumers from unfair and deceptive trade practices and addresses each situation as it arises.

The FTC has taken an active role in addressing data breaches and other data security concerns. It has chosen to take a flexible approach that encourages innovative solutions to security problems and data-based innovation more generally. Beginning in the late 1990s, the agency brought cases under its deception authority against websites who were not adhering to their own posted privacy policies.[9] In cases involving data breaches such as Wyndham and LabMD, the FTC has also relied on its unfairness authority.[10]

---

[3] Adam Thierer, "How Attitudes about Risk & Failure Affect Innovation on Either Side of the Atlantic," *Plain Text*, June 19, 2015.
[4] Andrea O'Sullivan, "How to Promote Data Privacy While Protecting Innovation," *The Bridge*, February 13, 2019.
[5] *FTC Informational Injury Workshop*.
[6] For a discussion of how an overly broad definition of covered entities can impact small businesses, see Will Rinehart, "Understanding the ADD Act," *American Action Forum*, January 17, 2019.
[7] Christopher Koopman et al., "Informational Injury in FTC Privacy and Data Security Cases" (Public Interest Comment, Mercatus Center at George Mason University, Arlington, VA, October 27, 2017).
[8] *Privacy & Data Security: Update: 2018* (Washington, DC: Federal Trade Commission, January 2018–December 2018).
[9] The first such action was Federal Trade Commission, "Geocities," February 12, 1999, https://www.ftc.gov/enforcement/cases-proceedings/982-3015/geocities.
[10] See FTC v. Wyndham Worldwide Corp., 799 F.3d 236 (3d Cir. 2015), alleging unfairness based on a lack of cybersecurity for customer information; see also LabMD, Inc. v. Federal Trade Commission, No. 1:1 4-CV-81o-WSD, 2014 WL 198716 (N.D. Ga. May

As a result of this case-by-case approach, the FTC has built a "common law of consent decrees" when it comes to data breaches and generally eschews more formal rulemaking or adjudication.[11] While this approach prevents many of the harms to innovation that could come from top-down rulemaking, it also lacks clear guidance for private actors who seek to remain compliant and creates uncertainty in what may arise if practices are challenged.[12] This lack of clarity has become an increasing issue in courts when entities challenge the FTC over its claims of unfairness or deception regarding data security. As Judge William S. Duffey Jr. stated when faced with LabMD data breach case, the FTC "ought to give [regulated parties] some guidance as to what you do and do not expect, what is or is not required. You are a regulatory agency. I suspect you can do that."[13]

Still, in general, this flexible approach of ex-post case-by-case enforcement has resulted in balancing the need for consumer redress with the benefits of innovation.[14] However, the FTC should strive to improve this approach through enforcement actions that develop a greater certainty around data security procedures that can protect consumers while continuing to avoid rigid, all-encompassing theories of harm that might actually deter future solutions and do little to nothing to improve the current state of data security.[15]

NARROWLY TAILORED SOLUTIONS IN LIGHT OF DATA BREACHES

Given the impracticalities and potential detriments of an overly broad theory of harm, there is still the possibility of narrowly tailored policy solutions to address the needs of particularly vulnerable data or persons.[16] As opposed to a broad, comprehensive approach, this narrowly tailored response has allowed innovative and popular uses of data to occur while still providing additional protection the data most likely to cause harm if breached, such as medical and financial information.[17] When considering how to address the potential concerns associated with credit reporting agencies, policymakers should be careful to contain such proposals to the specific circumstances of this industry.

Unlike most data interactions, consumers do not opt in and cannot opt out and pursue the services of other credit rating agencies. Similarly, the credit rating industry faces significant barriers to entry, so the regulatory impact on competition may be less significant if such regulations are tailored for this industry. Still, special caution should be paid to make sure that Congress does not grant unlimited, open-ended rulemaking authority to an agency, which could result in overly burdensome regulations beyond the credit reporting agencies.[18]

Regulation should not be seen as the only solution to data concerns even when dealing with such a specific area and sensitive information. Common law can play an important role when an individual can prove demonstrable harm, and this method has both adaptability and consistency well-suited to the current rapid pace of digital change.[19] While current law has not yet established a legal duty around data handling or privacy, existing precedents regarding tort and contract law place courts in an

---

7, 2014), involving an unfairness claim based on the accessibility of data after an employee had installed file-sharing software resulting in the data being accessible to third parties.

[11] Gus Hurwitz, "Data Security and the FTC's UnCommon Law," *Iowa Law Review* 101 (2016): 955–1022.

[12] Jennifer Huddleston, "Unprecedented: The Issue of Agency Action by Consent Order on Innovation," *Plain Text*, September 22, 2017.

[13] See the closing arguments at 8, LabMD, Inc., v. Federal Trade Commission, No. 9357 (F.T.C. Sep. 16, 2015).

[14] Koopman et al., "Informational Injury in FTC Privacy and Data Security Cases."

[15] Koopman et al.

[16] Jennifer Huddleston, *Preventing Privacy Policy from Becoming a Series of Unfortunate Events* (Washington, DC: American Action Forum, 2019).

[17] Huddleston, *Preventing Privacy Policy*.

[18] Jennifer Huddleston, "New GAO Report Says It's Time for Federal Data Privacy Legislation. But What Kind?," *The Bridge*, February 25, 2019.

[19] Jim Harper, "Remember the Common Law" (Cato Policy Report, Cato Institute, Washington, DC, March/April 2016).

appropriate position to determine when harm has occurred and when a duty has been reached without additional regulatory intervention.[20] Such an approach is more likely to be able to consider the specifics of the situation surrounding the breach, the information contained, and the reality of harm that may or may not have occurred as a result.

In addition to legislation and litigation, the importance of consumer choice and education should also not be neglected. While each of the 50 states has its own data breach notifications law, these laws vary both in terms of what information is covered and how and when affected consumers are to be informed, creating a complicated patchwork for both those companies experiencing a breach and consumers receiving notice.[21] As with other concerns about the current approach mentioned in these remarks, providing clarity and certainty over data breaches could benefit both consumers and innovators.

Finally, America should not forget the role consumers themselves can play in encouraging greater data security for sensitive information. As I noted in a previous comment with my colleagues Adam Thierer and Anne Hobson to the Consumer Product Safety Commission regarding potential risks associated with emerging internet of things technology, "Consumers, when they know about poor data security practices, can be effective advocates for change."[22] Consumer choice, consumer trust, and reputational risks can be powerful forces for encouraging solutions to data security problems.[23] Agencies and policymakers can play a complementary and educational role that allows consumers to make their own choices of next steps rather than assuming that they know the choices that consumers should make.

Concerns and issues around data security and data privacy are likely to continue to be part of the policy discourse. It is important to recognize that the use of data has many benefits both to current consumers and future technology. In considering the appropriate redress to troubling breaches, policymakers should be cautious and narrowly tailor their responses so as not to accidentally eliminate future successes in their drive to stop current failures. Thank you.

Sincerely,

Jennifer Huddleston
Research Fellow, Mercatus Center at George Mason University

[20] Koopman et al., "Informational Injury in FTC Privacy and Data Security Cases."
[21] Jennifer Huddleston, "Preventing Privacy Policy from Becoming a Series of Unfortunate Events," *American Action Forum*, January 14, 2019.
[22] Adam Thierer, Jennifer Huddleston, and Anne Hobson, "The Internet of Things and Consumer Product Hazards" (Public Interest Comment, Mercatus Center at George Mason University Arlington, VA, June 14, 2018).
[23] Thierer, Huddleston, and Hobson, "The Internet of Things."