MERCATUS CENTER
George Mason University

Bridging the gap between academic ideas and real-world problems

PUBLIC INTEREST COMMENT

INFORMATIONAL INJURY IN FTC PRIVACY AND DATA SECURITY CASES

CHRISTOPHER KOOPMAN
Director, Technology Policy Program, Mercatus Center at George Mason University

ADAM THIERER
Senior Research Fellow, Mercatus Center at George Mason University

ANDREA CASTILLO O'SULLIVAN
Program Manager, Technology Policy Program, Mercatus Center at George Mason University

JENNIFER HUDDLESTON SKEES
Legal Research Associate, Mercatus Center at George Mason University

Informational Injury Workshop P17-5413
Notice of Workshop and Opportunity for Comment
Agency: Federal Trade Commission
Proposed: September 29, 2017
Comment period closes: October 27, 2017
Submitted: October 27, 2017

INTRODUCTION

The Technology Policy Program of the Mercatus Center at George Mason University is dedicated to advancing knowledge about the effects of regulation on society. As part of its mission, the program conducts independent analyses to assess agency rulemakings and proposals from the perspective of consumers and the public. Therefore, this reply comment does not represent the views of any particular affected party but is designed to assist the agency as it explores these issues.

We appreciate the opportunity to submit reply comments regarding the Federal Trade Commission's (FTC) Workshop on Informational Injury. In her comments to the Federal Communications Bar Association on September 19, Chairwoman Maureen Ohlhausen defined the three goals of the workshop: (1) to "better identify the qualitatively different types of injury to consumers and businesses from privacy and data security incidents," (2) to "better explore frameworks for how we might approach quantitatively measuring such injuries and estimate the risk of their occurrence,"

For more information, contact
Canyon Brimhall, Outreach Associate, Technology Policy Program
703-993-8205, cbrimhall@mercatus.gmu.edu
Mercatus Center at George Mason University
3434 Washington Boulevard., 4th Floor, Arlington, VA 22201

and (3) to "better understand how consumers and businesses weigh these injuries and risks when evaluating the tradeoffs to sharing, collecting, storing, and using information."[1]

The workshop raises important and timely questions about the FTC's role in investigating cases relating to data breach and privacy incidents that fall within the commission's statutory unfairness and deception authorities.[2] Our comments will focus on developing a framework that appropriately addresses the ongoing challenges with data security without imposing on society an ineffective, all-encompassing theory of "harm" that may undermine the freedom to innovate in data use.

We begin with a discussion of data and security issues at the FTC. We then outline our vision for the future of FTC oversight of data breach cases, drawing heavily from the iterative process of common law. We then discuss why rigid theories of harm are inappropriate for meeting data security challenges. Finally, we provide a roadmap for how the commission can move closer to the ideal.

A BRIEF HISTORY OF THE FTC AND CYBERSECURITY

The United States currently lacks a dedicated regulator for data and security issues, allowing a number of agencies to become involved in cybersecurity issues relating to incidents in their primary jurisdictions. For example, the Securities and Exchange Commission issues guidance for financial institutions to safeguard their data, while the Food and Drug Administration has investigated device manufacturers for selling insecure medical devices. The FTC, however, is more involved than any other federal agency in data security oversight and adjudication.[3]

This was a development more of necessity than of design. As the internet revolution took hold in the 1990s and companies began grappling with new questions of data collection and storage, there was no regulatory framework to guide industry and establish legal certainty. The FTC, with its relatively broad Section 5 authority to protect consumers from deceptive or unfair acts or practices,[4] was well poised to fill the void.[5]

The commission initially promoted self-regulation as the primary policy for data and security issues,[6] a policy that would be supplemented by promotion of "fair information practice principles" as adequate standards to guide groups. However, the FTC quickly pivoted to more active measures in an attempt to promote internet security and thereby ensure its future functioning.[7] Specifically, the FTC first began pursuing potential privacy violations—where websites did not provide the level

[1] Maureen K. Ohlhausen, "Painting the Privacy Landscape: Informational Injury in FTC Privacy and Data Security Cases" (Speech before the Federal Communications Bar Association, Washington, DC, September 19, 2017).
[2] For a description of these authorities, see the FTC website at https://www.ftc.gov/about-ftc/what-we-do/enforcement-authority.
[3] Federal Trade Commission, *Privacy Online: Fair Information Practices in the Electronic Marketplace—A Report to Congress* (May 2000).
[4] 15 U.S.C. § 45 (2017).
[5] Woodrow Hartzog and Daniel J. Solove, "The Scope and Potential of FTC Data Protection," *George Washington Law Review* 83 (2015): 2230–2300.
[6] Federal Trade Commission, *Self-Regulation and Privacy Online: A Report to Congress* (July 1999).
[7] In 2000, the commission called upon Congress to pass comprehensive legislation expanding the government's role in controlling online privacy and data standards. This approach was ultimately unsuccessful, and several commissioners dissented against the recommendations provided to Congress. Michael D. Scott, "The FTC, the Unfairness Doctrine, and Data Security Breach Litigation: Has the Commission Gone Too Far?," *Administrative Law Review* 60, no. 1 (2008): 127–83.

of privacy promised in their stated privacy policies[8]—using a claim of "deception."[9] Later, the FTC became involved in matters relating to data breaches and security, applying its authority to investigate "unfairness" as a basis for such cases.[10] This approach has become controversial within academic and policy circles,[11] and it has spawned two notable legal battles.[12]

Despite lacking a specific congressional charge to oversee data and privacy issues, the FTC has persevered as the primary watchdog for consumer cybersecurity challenges.[13] Notably, as we discuss in more detail later, the FTC has largely eschewed an approach characterized by substantive rulemaking, favoring instead a quasi–common law method facilitated mainly by consent orders and administrative adjudication.[14] Furthermore, the FTC lacks a clear set of guidelines[15] to guide private actors who wish to both maintain good security and remain compliant with FTC best practices[16]—a situation that the commission admirably wishes to rectify with this very workshop.

While we applaud the FTC for its commitment to flexibility and its distaste for onerous, top-down regulation, we believe that the FTC should strive to get closer to a true common law approach rather than attempt to develop rigid, all-encompassing theories of harm that might keep lawyers busy but bring us no closer to better security and privacy. We outline a model path for the FTC to pursue in the following section.

THE COMMON LAW IDEAL

Concerns about existing tort law's ability to handle perceived intrusions into privacy are not new in the digital age. In fact, an 1890 *Harvard Law Review* article established the jurisprudence for privacy torts. Its authors—one of them, Louis D. Brandeis, would later become the famed associate justice of the Supreme Court—thought the rising power of newspapers and new technologies such as photography presented threats to individual privacy.[17]

---

[8] For example, the first of such FTC actions was *In re Geocities*, Docket No. C-3850 (F.T.C. February 5, 1999), where Geocities allegedly used user data in a way contrary to the guidelines laid out in Geocities's privacy policy.
[9] Steven Hetcher, "The FTC as Internet Privacy Norm Entrepreneur," *Vanderbilt Law Review* 53 (2000): 2041–61.
[10] Alden Abbott, "The Federal Trade Commission's Role in Online Security: Data Protector or Dictator?," The Heritage Foundation, September 10, 2014.
[11] Scott, "The FTC, the Unfairness Doctrine, and Data Security Breach Litigation."
[12] FTC v. Wyndham Worldwide Corp., 799 F.3d 236 (3d Cir. 2015); LabMD, Inc. v. Federal Trade Commission, No. 1:1 4 -CV-81o-WSD, 2014 WL 198716 (N.D. Ga. May 7, 2014).
[13] The FTC has undertaken at least 40 general privacy cases and 60 cases related to data security since 2002. Federal Trade Commission, *Privacy and Data Security—Update: 2016*, 2016.
[14] Gus Hurwitz, "Data Security and the FTC's UnCommon Law," *Iowa Law Review* 101 (2016): 955–1022.
[15] The FTC's public guidelines, called "Protecting Personal Information: A Guide for Business," provide general security tips, but no specific requirements for companies to follow. Rather, FTC officials have argued that parties must keep abreast of a byzantine maze of consent decrees to determine the extent to which their security practices are in line with FTC requirements. Federal Trade Commission, "Protecting Personal Information: A Guide for Business," October 2016.
16 Berin Szoka and Graham Owens, "FTC Stakeholder Perspectives: Reform Proposals to Improve Fairness, Innovation, and Consumer Welfare" (Testimony before the Subcommittee on Consumer Protection, Product Safety, Insurance, and Data Security of the US Senate Committee on Commerce, Science, & Transportation, September 26, 2017).
[17] Privacilla, *The Privacy Torts: How U.S. State Law Quietly Leads the Way in Privacy Protection*, July 2002.

Former FTC Chairwoman Edith Ramirez spoke positively of a common law approach to unfairness claims, stating that it is "well-suited to find the right balance [between flexibility and certainty]."[18] This statement is also true for the common law's ability to handle security-specific issues through existing privacy torts. Since legal scholar William L. Posser posited four common law privacy torts in 1960, most states have adopted and codified this typology through precedent or statute.[19]

Since relatively early in the digital era, these torts have evolved to accommodate reasonable expectations of privacy in cyberspace. The simultaneous adaptability and consistency of the common law gives it a clear advantage over statutory solutions.[20]

In the case of the informational harms proposed, courts have either handled or could handle these issues with existing tort law. For example, concerns about "dataveillance"—the monitoring of online activity—or other potentially deceitful injuries or subversions of consumer choice could be handled by applying intrusion into voluntary seclusion.[21] Intrusion is not necessarily physical in nature, so courts at common law can consider whether perceived online disclosures or other monitoring such as spyware can be challenged under the existing law.[22] Because the common law does not require a specific physical presence, the existing privacy torts can be extended and do not require an additional element of enforcement.

Some have expressed concerns that the anonymity and distance from the victim associated with using the internet or other technology to carry out intentional torts cause physical or financial harms that are not addressed by current privacy torts[23]; however, torts such as libel or intentional infliction of emotional distress do not require physical proximity to the victim as an element. Cyberspace may change the forum in which such acts are conducted, but it does not change the required elements. Moreover, the common law has evolved to account for situations when the alleged perpetrator remains anonymous through the use of internet platforms. Yelp has been forced to disclose the identities of anonymous reviewers when the reviews are found to be libelous, and individuals have been held liable for defamation or libel for fraudulent negative reviews.[24]

Courts are in a better position than regulators to determine when there is a legal duty in handling data and when that duty has been breached. Regulation is inflexible and preemptively shuts down

[18] Edith Ramirez, "Unfair Methods and the Competitive Process: Enforcement Principles for the FTC's Next Century" (Speech at the George Mason University School of Law, Arlington, VA, February 13, 2014).
[19] Privacilla, *The Privacy Torts*.
[20] Jim Harper, "Remember the Common Law" (Cato Policy Report, Cato Institute, Washington, DC, March and April 2016).
[21] Benjamin Zhu, "A Traditional Tort for a Modern Threat: Applying Intrusion upon Seclusion to Dataveillance Observations," *New York University Law Review* 89 (2014): 2401–2407.
[22] American Law Institute, *Restatement of the Law of Torts*, 2nd ed., § 652.
[23] See Mark MacCarthy, "New Directions in Privacy: Disclosure, Unfairness and Externalities," *I/S Journal of Law and Policy* 6 (2011): 425.
[24] Paresh Dave, "California Supreme Court to Review a Libel Case over Negative Yelp Reviews," *Los Angeles Times*, September 21, 2016); Kellan Howell and Phillip Swarts, "Yelp Critics Must Be Identified, Court Rules in Online Landscape Altering Decision," *Washington Times*, January 8, 2014).

potential avenues of innovation. In contrast, the courts are more flexible as they rule over specific contested avenues of innovation without curtailing other experiments.[25]

Currently, there is no established legal duty to handle most data or privacy in a certain way; however, a breach of terms of service or other data security claims could be handled under existing tort or contract law without additional regulatory intervention. The courts have been able to adapt existing common law torts of privacy to new media and technology in the past and should be able to adapt to current digital technology. Moreover, for the most vulnerable data, other statutory provisions already exist to establish a duty when handling the information. For example, the Health Insurance Portability and Accountability Act covers the duty surrounding medical information and data, the Children's Online Privacy Protection Act creates certain duties regarding data collected on children, and the Consumer Financial Protection Bureau's "unfair, deceptive, or abusive practices" standard can be employed against financial services companies for advertising false data management practices.[26]

A BAD ALTERNATIVE: A THEORY OF EVERYTHING

Chairwoman Ohlhausen has made it clear that the FTC is not seeking to "deduce a definition of injury from first principles."[27] Rather, she calls upon the community to consider (1) whether the FTC's current case-by-case approach toward privacy- and security-related "informational injury" is representative,[28] (2) whether any element may require government intervention, and (3) how the list of injuries corresponds with the FTC's statutory deception and unfairness authorities.[29]

We applaud the FTC for eschewing the temptation to develop a ground-up "theory of everything" to drive privacy and security oversight. Too often, members of the academy, the policy-making community, and the general public default to promoting jury-rigged, one-size-fits-all approaches toward concerns about public health and safety.[30] More thoughtful scholars, meanwhile, have attempted to sketch out an actionable rubric for informational harms and adequate remedies, to little avail or consensus.[31] We anticipate that the prominence of newsworthy data security incidents, particularly the recent compromise of Equifax's expansive personal finance datasets, will

---

[25] "Because the tort system operates retrospectively, it is restitution-based, not permission-based. This also creates incentives for firms to make their products safer over time so they can avoid lawsuits." Adam Thierer, *Permissionless Innovation: The Continuing Case for Comprehensive Technological Freedom*, 2nd ed. (Arlington, VA: Mercatus Center at George Mason University, 2016), 122.

[26] Consumer Financial Protection Bureau, "CFPB Takes Action against Dwolla for Misrepresenting Data Security Practices," March 2, 2016.

[27] Ohlhausen, "Painting the Privacy Landscape."

[28] The FTC currently groups its enforcement actions relating to privacy and security incidents into five categories: (1) deception injury, or subverting consumer choice, (2) financial injury, (3) health and safety injury, (4) unwarranted intrusion injury, and (5) reputational injury. Enforcement actions may be brought against individuals or groups if the harm caused to parties was inflicted through the FTC's authority to investigate unfair or deceptive practices. See Ohlhausen, "Painting the Privacy Landscape."

[29] Ohlhausen, "Painting the Privacy Landscape."

[30] For a specific critique of this approach as applied to online privacy standards, see Adam Thierer, "The Pursuit of Privacy in a World Where Information Control Is Failing," *Harvard Journal of Law and Public Policy* 36 (2013): 409–54.

[31] See, for example, M. Ryan Calo, "The Boundaries of Privacy Harm," *Indiana Journal of Law* 86 (2011): 1131–61; Joel R. Reidenberg, "Privacy Wrongs in Search of Remedies," *Hastings Law Journal* 877 (2003): 877–98; Daniel J. Solove, "A Taxonomy of Privacy," *University of Pennsylvania Law Review* 154, no. 3 (2006): 477–560.

fuel feedback to the FTC urging just this kind of approach. We suggest that the FTC stay the course in rejecting such calls for several reasons.

First, broadly defining informational harms could impose serious and unnecessary damage to the information economy. Europe has chosen to institute such a broad definition,[32] and the result has been to diminish competition and innovation in the EU information technology field.[33] Avoiding this approach will ensure that the United States remains a leader in information technology innovation.

Additionally, an expansive view of informational harms may conflict with First Amendment–protected speech. Scholars such as Eugene Volokh have pointed out that when the government determines an information privacy standard that extends into the private sector and prevents the sharing of information, it is inevitably silencing speakers.[34] This is not to say that restrictions on speech for privacy reasons are never allowed, but as with all limitations on free speech, such restrictions must be narrowly tailored.[35] The commission should draw on the current heightened standards for other speech-induced harms, such as defamation and libel, when considering restrictions on information sharing to ensure they do not risk unnecessarily limiting speech.

In practical terms, it is virtually impossible to develop and enforce a kind of overarching theory of harm appropriate for the internet age.[36] Opinions on what constitutes harm and appropriate redress are almost as varied as the number of people online, and different people have different risk thresholds.[37] In general, US regulators have eschewed this kind of approach, preferring instead to outline hard limits on certain behaviors—say, regarding child safety online—rather than attempting to pursue this Sisyphean task.

Furthermore, such attempts are simply unlikely to single-handedly improve security and privacy outcomes. Security is a fast-paced and dynamic space, and static frameworks will be ill suited to adapt to the evolving nature of developing threats. Similarly, 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. Smart policies require a degree of flexibility to best address both security and privacy.

How, then, can the FTC improve its privacy and security enforcement in a manner that addresses consumer needs without foisting an onerous and ineffective standard on private parties? The answer is by moving FTC enforcement closer to the ideal of common law evolution.

---

[32] Specifically, the EU's Data Protection Directive (DPD) of 1995 and General Data Protection Regulation (GDPR) of 2016 (to take effect in 2018) impose strict top-down regulations protecting a defined "right to privacy" in EU member states. The GDPR is even more expansive than the DPD, applying to companies not based in the EU that process data of EU residents. For more information, see Bert-Jaap Koops, "The Trouble with European Data Protection Law," *International Data Privacy Law* 4, no. 4 (2014): 250–61.

[33] Adam Thierer, "How Attitudes about Risk & Failure Affect Innovation on Either Side of the Atlantic," *Plain Text*, June 19, 2015; Larry Downes, "How Europe Can Create Its Own Silicon Valley," *Harvard Business Review*, June 11, 2015.

[34] Eugene Volokh, "Freedom of Speech and Information Privacy: The Troubling Implications of a Right to Stop People from Speaking about You," *Stanford Law Review* 52 (2000): 1088–89.

[35] Volokh, "Freedom of Speech and Information Privacy," 1106–22.

[36] Adam Thierer, "Online Privacy Regulation," Presentation to the Washington Legal Foundation, June 22, 2015.

[37] Daniel J. Solove, *Understanding Privacy* (Cambridge, MA: Harvard University Press, 2010).

BRIDGING THEORY AND PRACTICE: HOW THE FTC CAN IMPROVE

Chairwoman Ohlhausen notably characterized the FTC's current approach to privacy and security issues as common law–like. She described how the agency's "case-by-case enforcement . . . integrates feedback on earlier cases from advocates, the marketplace and, importantly, the courts. This ongoing process preserves companies' freedom to innovate with data use. And it can adapt to new technologies and new causes of injury."[38] The chairwoman's statements echo those of previous commissioner Julie Brill, who stated that the FTC's actions had created a "common law of privacy" in the United States.[39]

Unfortunately, the FTC's approach to privacy and security issues only superficially resembles a true common law path.[40] Rather than developing a real body of law through traditional litigation in the courts, the FTC has built up a mountain of loosely related consent orders[41] that all private parties must sift through to determine whether or not their businesses comply with FTC standards. Notably, this system operates in the absence of a defined rulemaking process; it does not include notice and comment, nor does it provide clear guidelines.[42]

Recent case law has shown the difficulty in applying an unclear standard of unfair or deceptive practices for both regulated entities and the courts. In the recent *LabMD* case,[43] for example, where the FTC attempted to bring action against a Georgia-based health laboratory despite a lack of notice or guidance, Judge William S. Duffey Jr. criticized the agency's approach to using consent orders to create regulation or duties without public awareness, stating that 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."[44]

Others have expressed similar frustration. In the *LabMD* case, the FTC attempted to launch a legal theory that had never been considered in court against the defendant, prompting FTC Chief Administrative Law Judge Michael Chappell to ask, "Where is the fairness in that, Counselor? If you're a company, you're a corporation, where is the fairness in a standard of what the law is being issued or published after the case is brought?"[45]

In *FTC v. D-Link*, the FTC claimed that firmware issues that made a router susceptible to hacking were an unfair and deceptive trade practice because they placed consumers' personal information

---

[38] Ohlhausen, "Painting the Privacy Landscape."
[39] Julie Brill, "Privacy, Consumer Protection, and Competition" (Speech before the 12th Annual Loyola Antitrust Colloquium, Loyola University Chicago School of Law, Chicago, IL, April 27, 2012).
[40] The following court cases are all cited in Hurwitz, "Data Security and the FTC's UnCommon Law."
[41] A consent order is an agreement between the FTC and a private party to settle a purported violation of an FTC rule or law under its authority. In entering into a consent order, the private party agrees to cease or correct the activity under FTC investigation.
[42] Szoka and Owens, "FTC Stakeholder Perspectives."
[43] It should be noted that the events preceding the action against LabMD are unusual, to put it charitably. A private intelligence firm called Tiversa apparently alerted the FTC that LabMD data was available on a P2P network sometime in 2010. LabMD disputes this version of events, claiming that Tiversa actually illegally accessed the data and passed it on to the FTC, creating the appearance of impropriety where there was none. Furthermore, LabMD alleged that Tiversa was actually in the pay of federal parties. Regardless of the intrigue surrounding the genesis of this action, the legal issues regarding notice and overreliance on consent decrees are more relevant for the purposes of this comment. For more information, see Evan M. Wooten and Lei Shen, "The Curious Case of LabMD: New Developments in the 'Other' FTC Data-Security Case," Mayer Brown, August 11, 2014.
[44] Closing Arguments at 8, LabMD, Inc., v. FTC, No. 9357 (F.T.C. Sep. 16, 2015).
[45] Transcript of Proceedings at 91, LabMD, Inc. v. FTC, No. 1:1 4 -CV-81o-WSD, 2014 WL 198716 (N.D. Ga. May 7, 2014).

and networks at risk.[46] A federal court for the Northern District of California found that while the FTC's claims that D-Link's comments about its security were sufficient to allow that portion of the case to continue, there was insufficient evidence to proceed under California's unfair trade practices law. The court also questioned the sufficiency of the claim regarding unfair trade practices under federal law.[47] The court dismissed the FTC's unfairness claims against D-Link for lack of an adequate injury, because the FTC did not "allege any actual consumer injury."[48] This shows at least that some courts will not allow the FTC to pursue a claim when there is no evidence that harm or injury has actually occurred.

FTC v. Wyndham Worldwide provides an example of how the FTC's current system not only fails to provide a common law itself, but complicates or confuses the existing common law with its lack of clarity. The FTC alleged that Wyndham hotels' lack of cybersecurity for consumer information, including credit card data and addresses, was an unfair practice when it was hacked, potentially exposing such information. The law is unclear about what constitutes an unfair practice for addressing data breaches, which in one case led the FTC to ask a district judge to take the unusual step of certifying the question to the Third Circuit on interlocutory appeal.[49] The Third Circuit affirmed the FTC's ability to use its Section 5 authority to enforce data security in the context of that litigation, but it questioned the lack of guidance provided for both the public and regulated individuals.[50] This struggle shows that the existing difficulties also prevent courts and common law from evolving their own definitions while the FTC standard remains notably vague.

Such concerns are not confined to the use of unfairness but also include the use of deception. Perhaps no case study illustrates this more clearly than *Nomi Technologies*.[51] Nomi collected shopping data and offered customers an option to opt out of both physical store data collection and website data collection. However, the data collection from physical stores was not successfully removed even when a consumer had opted out. Nomi served as a third-party contractor for the retailers in the collection of data and therefore, as Commissioner Ohlhausen stated in her dissent, had no obligation to provide consumers an opt-out.[52] By offering an option, however, the company was found to be deceptive despite having no duty to provide such an option and despite the lack of evidence of harm to any consumers. As some commenters at the time pointed out, the FTC's ruling made it better for an app developer not to provide any privacy policy rather than to provide one that may later prove to be flawed.[53] Not only does this ruling fail to provide clear standards for what constitutes deceptive practices for data privacy, it also punishes a company in the absence of consumer harm.

Rather than building on existing precedent to establish a series of understandable, stable norms, these orders and actions do little to clarify what the FTC considers an unfair or deceptive practice

[46] FTC v. D-Link Sys., No. 3:17-cv-00039-JD, at *2 (N.D. Cal. Sep. 19, 2017).
[47] *D-Link Sys.* at *3-*10.
[48] *D-Link Sys.* at *14.
[49] Hurwitz, "Data Security and the FTC's UnCommon Law."
[50] Federal Trade Commission v. Wyndham Worldwide Corp., 799 F.3d 236, 240, 257 n.23 (3d Cir. 2015).
[51] In the Matter of Nomi Technologies, Inc., FTC Matter No. 1323251, September 3, 2015.
[52] "Dissenting Statement of Commissioner Maureen K. Ohlhausen," In the Matter of Nomi Technologies, Inc., FTC Matter No. 1323251, April 23, 2015.
[53] Letter from Donald S. Clark, secretary of the Federal Trade Commission, to Michelle Lease et al., "Re: In the Matter of Nomi Technologies, Inc., File No. 1323251," August 28, 2015.

and fail to provide adequate guidance to regulated parties. Common law provides a precedent that regulated parties and individuals can build upon. The current system fails to adequately provide this guidance. The courts and current tort law may be better equipped to develop a system of common law to establish what duties are required.

Returning such issues properly to the courts as opposed to using administrative consent orders would not leave individuals without remedy and could provide better information to all involved. Class actions or individual lawsuits typically accompany or precede regulatory action. Courts have ruled that actual harm caused by the theft of personal information from a known data breach need not be proved; the heightened threat of identity theft from a "fairly traceable" data theft and the cost necessary to protect oneself from such risks following information exposure are sufficient to allow a case to proceed.[54] Courts are also able to provide injunctive relief to plaintiffs when necessary to stop further harm from occurring. While there is always a risk that common law could evolve in a less than ideal way, the risk of more consequential and restrictive regulations is far more likely to have a negative impact on both consumers and regulated industries.

Any regulation in this area should have a high bar of providing guidance that does not impact the continued development of new technology. It should also retain the right of both consumers and regulated entities to go to court and trust the common law instead of an administrative process.

CONCLUSION

In calling this workshop to examine the FTC's history and future of enforcement actions relating to privacy and security issues, the agency demonstrates that it recognizes feedback from industry and commentators and wishes to constructively improve upon its record. We applaud the FTC for recognizing this opportunity to improve, and we have outlined a framework that can maintain both consumer redress and regulatory flexibility.

We believe that the FTC and industry have the same goal: to protect consumers from informational harm without imposing a brittle bureaucratic structure that does little to promote actual security. To that end, we encourage the FTC to eschew any calls to develop rigid, all-encompassing theories of "informational injury" to guide future actions. Rather, the FTC should strive to develop a true body of common law precedent.

[54] Attias v. CareFirst, No. 16-7108 (D.C. Cir. Aug. 1, 2017) (allowing a class action concerning a data breach to go forward).