THE SCOPE AND POTENTIAL OF FTC DATA PROTECTION

This is an early draft, so please contact the authors before distributing or citing.

WOODROW HARTZOG[1]
Assistant Professor
Samford University's Cumberland School of Law

DANIEL J. SOLOVE[2]
John Marshall Harlan Research Professor of Law
George Washington University Law School

[1] Assistant Professor, Samford University's Cumberland School of Law; Affiliate Scholar, Center for Internet and Society at Stanford Law School.

[2] John Marshall Harlan Research Professor of Law, George Washington University Law School. The authors would like to thank the Law & Economics Center at the George Mason University School of Law for its support of this work.

INTRODUCTION

For more than fifteen years, the Federal Trade Commission (FTC) has regulated privacy and data security through its authority to police deceptive and unfair trade practices as well as through powers conferred by specific statutes and international agreements. Not until recently has the scope of the FTC's power to regulate privacy and data security been challenged. In *Federal Trade Commission v. Wyndham*,[3] a hotel chain has challenged the FTC's authority to regulate a company's data security practices. In *LabMD*[4], a medical diagnostics company raised similar objections as well as an assertion that in some contexts the FTC's data security authority is preempted by other statutory schemes.

These recent cases raise a fundamental issue, and one that has surprisingly not been well explored: How broad should the FTC's privacy and data security regulatory powers be? Is the FTC currently acting with the proper scope of its authority? Does it have room to expand its regulation? What are the real boundaries of FTC power? And normatively, should FTC regulation in the domain of data protection be contracted or expanded?

In this article, we address the issue of the scope of FTC authority over privacy and data security, which together we will refer to as "data protection" We argue that the FTC not only has the authority to regulate data protection to the extent it has been doing, but it also has the authority to expand its reach much more. Normatively, we argue that the FTC's current scope of data protection authority is essential to the United States data protection regime and should be fully embraced to respond to the privacy harms unaddressed by existing torts, contracts, and statutes.

In Part I, we discuss the legal boundaries of FTC data protection authority. We explore arguments made by critics of the FTC's data protection regulation that the FTC has been overstepping its authority in this domain. We respond by contending that the FTC's data protection authority has an intentionally broad scope. The FTC's authority under Section 5 of the FTC Act to regulate unfair and deceptive trade practices was designed precisely to avoid restrictive categories of practices which are unfair or deceptive. Additionally, Section 5's inevitable overlap with other statutes and regulatory domains is necessary and manageable. The FTC routinely shares regulatory authority with other administrative agencies. In response to the criticism that the FTC is engaging in a form of rulemaking in this area when it lacks meaningful rulemaking authority, we argue that anytime a broad standard is interpreted over time in a case-by-case adjudicatory manner, with an attempt to interpret consistently and treat prior decisions as having precedential value, the result will be the gradual calcification of the standard into a more rule-like structure. The FTC is not exceeding its authority because this developmental pattern is practically inevitable.

We argue that the FTC has been quite clear and consistent in its approach. For example, the FTC has based its data security jurisprudence on industry standards and a

[3] Opinion, FTC. Wyndham Worldwide Corp., Civil Action No. 13-1887 (ES), (D.N.J.), http://ashkansoltani.files.wordpress.com/2014/04/ftc-v-wyndham-opinion.pdf; First Amended Complaint for Injunctive and Other Equitable Relief, FTC v. Wyndham Worldwide Corp., No. 2:12-cv-01365-SPL (D. Ariz. filed Aug. 9, 2012) [hereinafter Wyndham Complaint], available at http://www.ftc.gov/os/caselist/1023142/index.shtm (on file with the authors); see also Julie Sartain, Analyzing FTC v. Wyndham, Int'l Ass'n of Privacy Professionals (Oct. 5 2012).

[4] In the Matter of LabMD, http://www.ftc.gov/enforcement/cases-and-proceedings/cases/2013/12/labmd-inc-matter.

reasonableness requirement instead of specific and rigid rules. Such an approach is more conservative than the FTC promulgating a set of standards all at once in a non-incremental manner. The standards evolve in a common law like fashion, a developmental pattern typical of the common law and the product of adherence to precedent, consistency in decisions, and case-by-case adjudication over time. In fact, if this pattern were not present, then the FTC would be acting inconsistently, ignoring previous actions, or reaching too far beyond particular cases.

In Part II, we turn to the normative issues regarding the scope of the FTC's data protection authority. We contend that the FTC currently serves as an essential lynchpin in the U.S. data protection regulatory regime. Curtailing the FTC's powers would severely upend the entire U.S. privacy regulatory regime. The U.S. privacy regulatory landscape developed as an amalgamation of various federal and state laws along with a significant amount of self-regulation. The FTC serves as a key lynchpin that holds everything together. The FTC is often the only regulator in town that has the resources to enforce necessary protections like data security. The FTC has served as a primary backbone for industry self-regulation, as it has added an essential enforcement component that has given self-regulation legitimacy and effectiveness. Moreover, the FTC also plays a pivotal role in international confidence regarding privacy in the United States. Loss of FTC privacy jurisprudence would threaten the existence the E.U. Safe Harbor agreement and other arrangements that govern the international exchange of personal information.

We contend that the FTC is able to balance data protection against countervailing interests in ways that other areas of law are currently unable to do. Contract law and tort law have thus far not been frequently applied to many of the issues involving the collection, storage, use, and disclosure of personal data. More broadly, the law has struggled to recognize privacy violations and data security breaches as harms. The FTC can regulate with a much different and more flexible understanding of harm that one focused on monetary or physical injury. According to the FTC, even incremental harms that affect a large group of consumers can be substantial.

We argue that the FTC has the authority to expand its data protection regulation and that it should do so. The FTC's broad authority to regulate unfair and deceptive acts is well suited to incrementally develop a robust regime to tackle the privacy challenges wrought by new technologies. So far, the FTC has developed its jurisprudence in a very measured and modest way. We argue that the FTC can and should push in bolder and more aggressive directions, which might be necessary as Big Data, the Internet of Things, data brokers, and other challenges continue to vex courts and lawmakers. As a nimble agency capable of directly and indirectly regulating both relationships and design, the FTC is the ideal authority to police a landscape fraught with uncertainty.

In Part III, we explore the limits of the FTC's Section 5 authority over data protection. Materiality, balancing, and harm requirements facially limit the scope of valid complaints. There are some types of harm, such as purely emotional ones, that are better suited to the purview of torts and contracts. Compensatory remedies are also better suited for torts or other statutes because the FTC's role is largely to discourage bad behavior. The FTC also operates under significant resource constraints, and has generally brought only about ten to twenty five privacy and data security cases per year. The FTC is also subject to political pressure. So there is good reason not to completely abandon the panoply of other remedies for privacy harms.

For the FTC to continue in its current role regarding data protection and for it to expand this role, it must make some changes in the way it exercises its power. Although the FTC has provided a fair amount of notice to organizations, it can and should do more to inform companies of their obligations under Section 5. If the FTC is to fully embrace its role as a data protector using the case-by-case approach, it should not only provide more detail in its complaints but also in the quantity and substance of closing letters issued when an investigation does not lead to a complaint. The FTC should also try to encourage better data protection practices by avoiding a uniform approach to enforcement. Instead, the agency should seek milder punishments and shorter auditing periods from companies that significantly protected data and made a good faith attempt at compliance, yet still ran afoul of Section 5.

Ultimately, we contend that far from being too broad and bold in its authority, the FTC is currently too measured and conservative. Political considerations and the newness of privacy and data security issues may justifiably explain the FTC's modest approach. But now data protection has matured into a more robust field, with more developed industry norms as well as a much more significant understanding of the issues among practitioners and the academy. The magma has settled and started to cool, and the foundations are present for the FTC to step further into its developing role as the de facto U.S. data protection agency.

I. THE BOUNDARIES OF FTC POWER

In the 1990s, the Internet was blossoming and concerns about privacy and data security were mounting. Despite a few laws regulating certain industries, much of online commerce and much of the collection and use of personal data more generally were regulated primarily by self-regulation.[5]

Enter the FTC. The agency had long been focused on consumer protection, which it enforced through its powers under Section 5 of the FTC Act. Under this statute, "unfair or deceptive acts or practices in or affecting commerce, are hereby declared unlawful."[6] The FTC began its foray into privacy and data security 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.[7]

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. By "data

[5] *See, e.g.*, Michael D. Scott, The FTC, the Unfairness Doctrine, and Data Security Breach Litigation: Has the Commission Gone Too Far?, 60 Admin. L. Rev. 127, 130 (2008) ("The FTC initially sought to deal with online privacy issues by encouraging industry self-regulation.") (citing Federal Trade Commission, Privacy Online: A Report to Congress Fair Information Practices in the Electronic Marketplace 3 (May 2000), available at http://www.ftc.gov/reports/privacy2000/privacy2000.pdf; Federal Trade Commission, Privacy Online: A Report to Congress 2 (June 1998), available at http://www.ftc.gov/reports/privacy3/priv-23a.pdf Federal Trade Commission, A Report from the Federal Trade Commission Staff: The FTC's First Five Years Protecting Consumers Online (Dec. 1999), available at http:// www.ftc.gov/os/1999/12/fiveyearreport.pdf).

[6] 15 U.S.C. § 45(a)(1).

[7] Daniel J. Solove and Woodrow Hartzog, The FTC and the New Common Law of Privacy, 114 Colum. L. Rev. 583 (2014), available at http://ssrn.com/abstract=2312913.

protection," we are referring broadly to issues involving the privacy (collection, use, and disclosure) and security (administrative, technical, and physical safeguards) of personal data. 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.[8] The FTC soon uncoiled its power to police unfair trade practices and began bringing claims.

Today, the FTC has evolved into the broadest and most powerful data protection agency in the United States. No other agency has such a broad scope of power over so many different industries. For example, the Department of Health and Human Services is limited to regulating entities subject to HIPAA.[9] Although there are a broad array of HIPAA-regulated entities, countless industries do not fall under HIPAA. The Federal Communications Commission has jurisdiction over telecommunications, satellite, broadcast, and cable companies, but its range does not extend much further.[10]

In contrast, the FTC's scope covers nearly any for-profit entity that handles personal data. Except for a few small industry carve-outs, nearly every industry is subject to FTC enforcement power, including industries such as automotive, financial, health, retail, online services, hospitality, entertainment, manufacturing, data processing, food and beverage, transportation, and many more.[11] Any industry where consumers are involved is typically within the scope of FTC enforcement power.

This broad grant of authority was designed precisely to avoid restrictive categories of practices which are unfair or deceptive.[12] As the FTC has taken a greater foothold in the data protection arena, critics have pushed back, raising concerns over the proper scope of the FTC's power. For example, Wyndham Hotels has argued:

> [The FTC] asserts a staggeringly broad theory of agency power. . . .The FTC believes that it can engage in such regulation without publishing any rules or regulations explaining in advance what companies must do to comply with the law. Instead, the FTC can provide no notice at all and bring "case-by-case" enforcement actions against companies that have suffered cyber attacks. . . . Such an Orwellian understanding of governmental power is so foreign to our system of justice that Congress could not possibly have intended the FTC to wield it.[13]

---

[8] *Id.*

[9] 42 U.S.C.A. § 1320d–2. Section 264(a).

[10] 47 U.S.C.A. §§ 151-216b (West); What We Do, Federal Communications Commission, http://www.fcc.gov/what-we-do ("The Federal Communications Commission regulates interstate and international communications by radio, television, wire, satellite and cable….").

[11] According to Section 5 of the FTC Act, the specific carve outs of FTC jurisdiction are "banks, savings and loan institutions described in section 57a (f)(3) of this title, Federal credit unions described in section 57a (f)(4) of this title, common carriers subject to the Acts to regulate commerce, air carriers and foreign air carriers subject to part A of subtitle VII of title 49, and persons, partnerships, or corporations insofar as they are subject to the Packers and Stockyards Act, 1921." 15 U.S.C. § 45(a)(2).

[12] *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").

[13] Reply in Support of Motion to Dismiss by Defendant Wyndham Hotels & Resorts LLC, FTC v. Wyndham Worldwide Corp., Case No. CV 12-1365-PHX-PGR, at 2; *see also* Brief of Amici Curiae Chamber of Commerce of the United States of America, Retail Litigation Center, and American Hotel and & Lodging Association in Support of Defendants, FTC v. Wyndham Worldwide Corp., Case No. CV 12-1365-PHX-PGR ("The FTC has overreached. It lacks the legal authority to act as a roving regulator of data security standards, because the statute under which the FTC has purported to act – Section 5 of the FTC Act – does not authorize the Commission to proceed as it has in this case.").

Wyndham and others fault the FTC for enforcing in many areas also enforced by other agencies. For example, in the LabMD case, LabMD also is subject to enforcement by the HHS Office for Civil Rights (OCR).[14] The FTC also enforces in areas regulated by other federal and state statutes, such as data breach notification laws and others.

How broad is the FTC's authority? Has it exceeded appropriate bounds? Is it encroaching upon areas that should be the exclusive domain of other agencies? What are the proper boundaries? In this Part, we examine the arguments by critics of the FTC that it has pushed beyond the proper scope of its enforcement authority. We then examine just how large the FTC's boundaries actually are.

A. The Critiques of the FTC's Data Protection Authority

The *Wyndham* case is the first and one of the most significant challenges to the FTC's data protection power to date. In that case, the FTC alleged that Wyndham, a company that manages hotels and sells timeshares, suffered a series of three breaches using similar techniques to access personal information stored on the Wyndham-branded hotels' property management system servers, including "customers' payment card account numbers, expiration dates, and security codes."[15]

The FTC claimed that "[a]fter discovering each of the first two breaches, Defendants failed to take appropriate steps in a reasonable time frame to prevent the further compromise of the Hotels and Resorts' network." According to the FTC, more than 619,000 people's payment card account numbers were compromised, and "consumers and businesses suffered financial injury, including, but not limited to, unreimbursed fraudulent charges, increased costs, and lost access to funds or credit. Consumers and businesses also expended time and money resolving fraudulent charges and mitigating subsequent harm."

The FTC claimed that Wyndham deceptively stated in its privacy policy that it protected its customers' personal information by using "industry standard practices" and "a variety of different security measures designed to protect personally identifiable information from unauthorized access by users both inside and outside of our company." Other allegedly deceptive statements included a promise that Wyndham takes "commercially reasonable efforts to create and maintain 'fire walls' and other appropriate safeguards to ensure that to the extent we control the Information, the Information is used only as authorized by us and consistent with this Policy, and that the Information is not improperly altered or destroyed." The FTC alleged that Wyndham actually provided deficient data security practices contrary to their representations of following "industry standard practices."

In addition to claiming deceptiveness, the FTC also faulted Wyndham's data security practices on unfairness grounds. Specifically, the FTC identified practices that "unreasonably and unnecessarily exposed consumers' personal data to unauthorized

[14] See, e.g., 42 U.S.C. § 1320d2(d)(1).

[15] First Amended Complaint for Injunctive and Other Equitable Relief, FTC v. Wyndham Worldwide Corp., No. 2:12-cv-01365-SPL (D. Ariz. filed Aug. 9, 2012) [hereinafter Wyndham Complaint], available at http://www.ftc.gov/os/caselist/1023142/index.shtm (on file with the authors).

access and theft." Among other things, the FTC alleged that Wyndham failed to use readily available access guards (firewalls), allowed misconfiguration, resulting in storage of credit card information in clear text, failed to ensure implementation of adequate security policies before connecting to main network, failed to remedy known security vulnerabilities (for example by connecting insecure serves without outdated OS unable to get security patches). Wyndham also allowed computers with well-known default IDs to connect to network, failed to make passwords hard to guess, failed to inventory networked computers, and failed to employ reasonable measures to detect, prevent unauthorized access, failed to follow proper incident response procedures, including monitoring for malware post breach, and failed to adequately restrict third-party vendor access.

Unlike nearly all other defendants in an FTC action, Wyndham did not settle with the FTC. Instead, it brought an action in federal court.

On April 7, 2014, the United States District Court for the District of New Jersey issued its long-awaited opinion in the case.[16] The court rejected Wyndham's calls to create a data security exception to the FTC's broad authority to regulate unfair practices under Section 5 of the FTC Act. The court also rejected Wyndham's assertion that the FTC must formally promulgate regulations before bringing an unfairness claim as well as Wyndham's argument that the FTC failed to provide fair notice of what constitutes an unfair data security practice.

Wyndham made three principal arguments related to the scope of the FTC's unfairness authority in its motion to dismiss: (1) The FTC unfairness authority does not extend to data security; (2) The FTC has failed to give fair notice of what data security practices are required by law, and (3) Section 5 does not apply to the security of payment card data because there is no possibility for consumer injury. U.S. District Judge Salas resolved each of these issues in favor of the FTC and denied Wyndham's motion to dismiss.

Regarding the scope of the FTC's Section 5 authority, Wyndham asserted that the "overall statutory landscape" made it clear that unfairness authority does not extend to data security. For example, Wyndham noted that Congress has enacted targeted data security legislation elsewhere yet failed to create a statute explicitly authorizing the FTC to regulate data security. Relying on *FDA v. Brown & Williamson Tobacco Corp.*,[17] Wyndham argued that these targeted statutes demonstrated that the FTC lacked broader authority to regulate in this area.

Wyndham also argued that, like the FDA in *Brown & Williamson*, the FTC disclaimed authority to regulate data security under Section 5's unfairness prong. Judge Salas, however, rejected the comparison: "[T]he Court is not convinced that these statements, made within a three-year period, equate to a resolute, unequivocal position under *Brown & Williamson* that the FTC has *no* authority to bring *any* unfairness claim involving data security."[18] The court noted that the FTC actually "brought unfairness claims in the data-

[16] FTC v. Wyndham Worldwide Corp., No. 13-1887 Slip Op. (April 7, 2014 D.N.J.)
[17] 529 U.S. 120 (2000).
[18] *Id.* at 13 (emphasis in original).

security context shortly after these representations. And the FTC's subsequent representations confirm its authority in this arena, not deny it."[19]

Regarding fair notice, Wyndham argued that the FTC must "set data-security standards in advance, so that businesses can fairly know what is required of them before the FTC seeks to hold them liable."[20] The company also argued that the FTC failed to articulate exactly what the vague standards created by use of the terms "reasonable," "adequate," or "proper" require.

The FTC disagreed with Wyndham's argument that rulemaking is the only proper way for the FTC to regulate data security. According to the FTC, rulemaking would be inappropriate because data security is highly contextual and always changing. Regarding defining what "reasonable" security is, the FTC argued that companies can look to a few things for guidance: "(1) industry guidance sources that [Wyndham] itself seems to measure its own data-security practices against; and (2) the FTC's business guidance brochure and consent orders from previous FTC enforcement actions."[21]

The FTC also asserted that data-security standards can be enforced in an industry-specific, case-by-case way, analogizing its strategy in regulating data security with the approach of other agencies who bring actions without "particularized prohibitions" such as the National Labor Relations Board (NLRB) and the Occupational Safety and Health Act (OSHA).

Regarding injury, Wyndham argued that federal statutes and card-brand rules eliminate the possibility that consumers can suffer financial injury from the theft of payment-card data. Wyndham also rejected the notion that "incidental injuries that consumers suffered" such as the cost of remedial finance monitoring was insufficient to constitute a "substantial injury." Wyndham rejected the FTC's interpretation that consumer injury can include the aggravation, time, and effort associated with obtaining reimbursement from card issuers and otherwise responding to a data breach.

On the heels of Wyndham, another defendant challenged the FTC's Section 5 enforcement authority. In *LabMD*, the FTC brought a complaint against a medical testing laboratory alleging that the company "failed to reasonably protect the security of consumers' personal data, including medical information."[22] In a press release, the FTC described their complaint as alleging "that in two separate incidents, LabMD collectively exposed the personal information of approximately 10,000 consumers." The FTC asserted that "LabMD billing information for over 9,000 consumers was found on a peer-to-peer (P2P) file-sharing network and then, in 2012, LabMD documents containing sensitive personal information of at least 500 consumers were found in the hands of identity thieves."[23] The FTC claimed that this failure to "employ reasonable and appropriate measures to prevent unauthorized access to personal information, including

[19] *Id.*
[20] FTC v. Wyndham Worldwide Corporation, et. al., Defendants., 2012 WL 5388693 (D.Ariz.).
[21] *Id.* at 17.
[22] FTC Files Complaint Against LabMD for Failing to Protect Consumers' Privacy , FTC.gov (August 29, 2013), http://www.ftc.gov/news-events/press-releases/2013/08/ftc-files-complaint-against-labmd-failing-protect-consumers .
[23] *Id.*

dates of birth, SSNs, medical test codes, and health information," was an unfair practice.[24]

In its motion to dismiss, LabMD made similar arguments to those made by Wyndham. It asserted that the FTC lacks the authority under a Section 5 unfairness theory to regulate patient information security practices and that the FTC has failed to provide fair notice of what data security practices it believes Section 5 requires. One additional argument unique to LabMD was that only HHS, and not the FTC, has the authority to regulate data security practices affecting patient data regulated by HIPAA.[25]

Although *Wyndham* and *LabMD* involve data security issues, the import of their arguments extend to the whole domain of data protection, including privacy. Essentially, the arguments boil down to whether Section 5 authority can extend into areas regulated by other laws, whether the FTC can continue in its case-by-case fashion in developing data protection jurisprudence, and whether the FTC is exercising unfairness authority in areas without clear consumer harm.

Beyond Wyndham and LabMD, various commentators have attacked the FTC for overreaching. Regarding data security, Michael Scott has argued that the FTC's data security complaints were "seemingly filed at random, without any guidelines, and without any advance notice to the respondents that their actions might violate § 5 of the FTC Act. The complaints and consent orders entered into in these cases provide limited guidance as to what a company should do (or not do) to avoid being the target of an unfairness action by the FTC if it experiences a security breach."[26] Similarly, Berin Szoka and Geoff Manne have contended that "At the heart of the discretionary model is the FTC's ability to operate without any real constraints. The Commission hasn't developed a predictable set of legal doctrines because that's what courts do — and the FTC has managed to strong-arm dozens of companies into settling out of court. What the FTC calls its 'common law of consent decrees' is really just a series of unadjudicated assertions."[27]

In an amicus brief filed in *Wyndham*, TechFreedom, the International Center for Law & Economics, Berin Szoka, Geoff Manne and several other scholars including Gus Hurwitz, Tood Zywicki, and Paul Rubin argue that the "FTC's current approach to data security denies companies like Wyndham 'a reasonable opportunity to know what is prohibited' and thus follow the law."[28]

Gerry Stegmaier and Wendell Bartnick similarly argue that "although the FTC has undertaken significant efforts to develop and improve notice of its interpretation of Section 5, the nature, format, and content of the agency's data-security-related

---

[24] Complaint, In the Matter of LabMD, http://www.ftc.gov/sites/default/files/documents/cases/2013/08/130829labmdpart3.pdf.

[25] *Id.*

[26] Michael D. Scott, The FTC, the Unfairness Doctrine, and Data Security Breach Litigation: Has the Commission Gone Too Far?, 60 Admin. L. Rev. 127, 183 (2008).

[27] Berin Szoka and Geoffery Mane, The Second Century Of The Federal Trade Commission, Techdirt (Sept. 26, 2013), http://www.techdirt.com/blog/innovation/articles/20130926/16542624670/second-century-federal-trade-commission.shtml.

[28] Amici Curiae Brief of TechFreedom, International Center for Law and Economics & Consumer Protection Scholars, FTC v. Wyndham Worldwide Corp. No. 2:12-cv-01365-SPL (D. Ariz. filed June 17, 2013), http://docs.techfreedom.org/Wyndham_Amici_Brief.pdf.

pronouncements raise equitable considerations that create serious due process concerns."[29] The authors ask, "If an entity cannot ascertain what the law is, how can it know what it must do—especially where liability most commonly arises out of the malfeasance of others?"[30]

Other critics assail the FTC for enforcing when there is not sufficient consumer harm. According to James Cooper, "the harms associated with the FTC's privacy agenda are largely subjective and intangible, often boiling down to little more than the creepy feeling of being tracked online."[31]

Critics like Szoka and Manne have not completely rejected the FTC as a viable privacy regulator, however, particularly when compared to potentially static legislation. Regarding Facebook's settlement with the FTC of complaints over allegedly deceptive privacy-related statements, Szoka stated, "Case-by-case adjudication is a venerable American tradition—one that's more, not less, vital in the rapidly changing field of consumer privacy. Rather than rushing to write new laws, Congress should focus on ensuring the FTC has the resources it needs to use its existing authority effectively. That means, most of all, having a larger core of technologists on staff to guide what is supposed to be our expert agency on privacy."[32]

Szoka and Manne elsewhere stated, "When Congress created the Federal Trade Commission ninety-nine years ago today, it never imagined the Commission would become the primary agency responsible for grappling with technological change, but that's precisely what the FTC has become: the de facto Federal Technology Commission. In principle, this is mostly for the best. The FTC's case-by-case approach is far better suited to fast-changing industries, from broadband to Uber to data-driven tech companies, than the FCC, local taxicab commissions or European-style data protection agencies."[33] To Szoka and Manne, while the case-by-case approach is good in theory, they argue that "how the agency works is deeply problematic."[34] Szoka and Manne argue that "neither this 'common law of consent decrees' nor the FTC's privacy reports constitute actual law. It's a flexible approach, but only in the worst sense: made by disposing of any legal constraints or due process."[35] As we explore below, the FTC is actually bound by many constraints including due process. While the FTC's jurisdictional reach and discretion are quite broad, this is by design.[36] Moreover, it is precisely this broad scope that makes the FTC the most critical organization in the U.S. privacy regulatory ecosystem.

B. The Scope of FTC Authority

---

[29] Gerard M. Stegmaier and Wendell Bartnick, Psychics, Russian Roulette, and Data Security: The Ftc's Hidden Data-Security Requirements, 20 Geo. Mason L. Rev. 673, 676 (2013).
[30] *Id.*
[31] James C. Cooper, *Identity Theft, Not Big Data, Should Be At the Top of the FTC's Priority List,* The Daily Caller (Sept. 24, 2013), http://dailycaller.com/2013/09/24/identity-theft-not-big-data-should-be-at-the-top-of-the-ftcs-priority-list/#ixzz2fwIBwOnY.
[32] Szoka Statement on Facebook FTC Privacy Settlement, TechFreedom (Noc. 29, 2011), http://techfreedom.org/post/58365342326/szoka-statement-on-facebook-ftc-privacy-settlement.
[33] Now in its 100th year, the FTC has become the Federal Technology Commission, TechFreedom (Sept. 26, 2013), http://techfreedom.org/post/62344465210/now-in-its-100th-year-the-ftc-has-become-the-federal.
[34] *Id.*
[35] *Id.*
[36] For example, the FTC has wide discretion as to which actor the FTC file s complaint against and is not required to pursue worst actors or any actor in particular. Moog Industries, Inc. v. FTC - 355 U.S. 411 (1958).

Contrary to some critics, the FTC enjoys a very extensive data protection enforcement authority. Indeed, the scope of its authority is intentionally broad. The legislative history of Section 5 demonstrates a clear intent that the FTC's authority be evolutionary and wide-reaching.

1. The Broad Concepts of Deception and Unfairness

As noted by Judge Salas in Wyndham, the concepts of deceptiveness and unfairness in the FTC Act are intentionally defined at an extremely broad level. Rather than attempt to define the specific consumer protection issues that the FTC should focus on, Congress created two broad categories – practices that are deceptive and unfair– with virtually no hard boundary lines. Critics of the FTC in the Wyndham case point to legislative modifications of the FTC's authority as evidence of Congressional intent that the FTC be highly constrained, but this argument is misplaced.[37] Yet even in light of the limitations imposed by Congress and earlier clarifying statements on deception and unfairness, the FTC's authority remains explicitly general and expansive.[38]

The scope of the FTC's deceptiveness jurisdiction is far-reaching. Any material representation, omission or practice that is likely to mislead a reasonable consumer is actionable.[39] This includes 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.[40] 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.[41]

Thus, the FTC's deception authority extends far beyond policing privacy policies. Although enforcing privacy policy promises was how the FTC began its foray into the area, the concept of deception under Section 5 is much broader.

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

[37] Brief of Amici Curiae Chamber of Commerce of the United States of America, Retail Litigation Center, and American Hotel and & Lodging Association in Support of Defendants, FTC v. Wyndham Worldwide Corp., Case No. CV 12-1365-PHX-PGR at 8 ("Thirty years ago, the FTC sought to significantly expand the scope of its Section 5 authority, invoking the then-extant version of the statute to advance its consumer protection goals in ways far beyond those envisioned by Congress. Congress reacted to that overreach, codifying into law significant limits on the scope of the FTC's authority.").

[38] Federal Trade Commission Act Amendments of 1994, Pub. L. No. 103-312, 108 Stat. 1691 (1994) (codified at 15 U.S.C. § 45(n)); FTC Policy Statement on Unfairness, Appended to International Harvester Co., 104 F.T.C. 949, 1070 (1984). See 15 U.S.C. § 45(n); FTC Policy Statement on Deception , Appended to Cliffdale Associates, Inc., 103 F.T.C. 110, 174 (1984).

[39] *See* FTC Statement on Deception, Appended to Cliffdale Associates, Inc., 103 F.T.C. 110, 174 (1984).

[40] Daniel J. Solove and Woodrow Hartzog, The FTC and the New Common Law of Privacy, 114 Colum. L. Rev. 583 (2014) (draft of Aug. 19, 2013), available at http://ssrn.com/abstract=2312913.

[41] *Id.*

become outdated or leave loopholes for easy evasion."[42] Notably, the FTC can find a practice unfair even when it is otherwise legally permissible.[43]

Regarding the meaning of unfairness, the House Conference Report famously stated: "It is impossible to frame definitions to embrace all unfair practices. There is no limit to human inventiveness in this field. Even if all known unfair practices were specifically defined and prohibited, it would be at once necessary to begin over again. If Congress were to adopt the method of definition, it would undertake an endless task."[44] Thus, it is the FTC that is responsible, subject to judicial review, for identifying unfair trade practices.

In its statement on unfairness, the FTC cited the Supreme Court's explicit recognition that unfairness need not be defined ex ante, instead growing through evolution.[45] The Court stated that the term unfairness ""belongs to that class of phrases which do not admit of precise definition, but the meaning and application of which must be arrived at by what this court elsewhere has called 'the gradual process of judicial inclusion and exclusion."[46] The U.S. Court of Appeals for the Second Circuit stated with respect to unfairness, "The Commission has a wide latitude in such matters; its powers are not confined to such practices as would be unlawful before it acted; they are more than procedural; its duty in part at any rate, is to discover and to make explicit those unexpressed standards of fair dealing which the conscience of the community may progressively develop."[47]

The recent opinion in *Wyndham* supports this view. Judge Salas rejected Wyndham's argument that the FTC does not have the authority to regulate data security. Instead, Judge Salas concluded that the FTC has broad power under Section 5 to support its exercise of authority, and the context-specific data security statutes simply enhance data security authority in certain contexts by removing consumer injury requirements, granting the FTC additional enforcement powers that it otherwise lacks, and affirmatively compelling (rather than merely authorizing) the FTC to use its authority in particular ways.

Judge Salas wrote that Wyndham "fails to explain how the FTC's unfairness authority over data security would lead to a result that is incompatible with more recent legislation

---

[42] FTC Policy Statement on Unfairness, Appended to International Harvester Co., 104 F.T.C. 949, 1070 (1984). See 15 U.S.C. § 45(n).

[43] Spiegel v. FTC, 540 F.2d 287, 292 (1976) (citing FTC v. Sperry & Hutchison, Co., 405 U.S. 233 (1972)) ("[T]he Supreme Court left no doubt that the FTC had the authority to prohibit conduct that, although legally proper, was unfair to the public.").

[44] FTC v. Sperry and Hutchinson, supra at 240 (quoting from House Conference Report No. 1142, 63 Cong., 2d Sess., 19 (1914)).

[45] *Id.* (citing FTC v. Raladam Co., 283 U.S. 643, 648 (1931). See also FTC v. R.F. Keppel & Bro., 291 U.S. 304, 310 (1934) ("Neither the language nor the history of the Act suggests that Congress intended to confine the forbidden methods to fixed and unyielding categories")).

[46] *Id.*

[47] FTC v. Standard Education Society, 86 F.2d 692, 696 (2nd Cir. 1936) rev'd on other grounds 302 U.S. 112 (1937). Courts have explicitly given significant deference to the FTC's interpretations of what constitutes an unfair or deceptive trade practice. *See* Earl Kinter & William Kratzke, Federal Antitrust Law § 43.65 ("[T]he courts have declared an intention to give wide discretion to the Federal Trade Commission to declare acts or practices unfair, but certainly this is not a discretion the Commission cannot overstep, notwithstanding the increasing deference to agency interpretation skills.").

and thus would 'plainly *contradict* congressional policy.'"[48] In other words, because Congress's actions all seem to complement, not preclude, the FTC's authority over data security, this dispute is not similar to the FDA's repudiated authority over tobacco products at issue in *Brown & Williamson*.

In a recent order denying LabMD's motion to dismiss, Commissioner Josh Wright, writing for a unanimous Commission, confirmed the FTC's authority to enforce the FTC Act by adjudicating whether data security practices are unfair. The order stated, "Congress, in enacting Section 5(n), confirmed its intent to allow the Commission to continue to ascertain, on a case-by-case basis, which specific practices should be condemned as 'unfair.'"[49] Citing previously cases, the Commission noted that "to this day, 'Congress has not at any time withdrawn the broad discretionary authority originally granted the Commission in 1914 to define unfair practices on a flexible, incremental basis.'"[50] It observed that "[t]he Commission and the federal courts have been applying these three "unfairness" factors for decades and, on that basis, have found a wide range of acts or practices that satisfy the applicable criteria to be "unfair," even though – like the data security practices alleged in this case – 'there is nothing in Section 5 explicitly authorizing the FTC to directly regulate" such practices.'"[51]

The concept of unfairness is thus quite intentionally broad and subject to refinement over time. Instead of specific categories, the FTC's unfairness authority is limited to instances where there is an actual or likelihood of unavoidable harm which is not outweighed by countervailing benefits to consumers or competition.[52]

An exceptionally wide range of activities have been included in the FTC's unfairness and regulatory efforts, including creating a physical danger to children,[53] high pressure sales environments,[54] the unilateral imposition of fees in breach of a service contract,[55] and failure to disclose substantial risk of physical injury from hazardous exercise equipment.[56] Stephen Calkins stated, "Modern Commission unfairness cases fall into five categories: (1) theft and the facilitation thereof (clearly the leading category); (2) breaking or causing the breaking of other laws; (3) using insufficient care; (4) interfering with the exercise of consumer rights; and (5) advertising that promotes unsafe

[48] FTC v. Wyndham Worldwide Corp., No. 13-1887 Slip Op. (April 7, 2014 D.N.J.) at 10.
[49] Order Denying Respondent LabMD's Motion to Dismiss, In the Matter of LabMD, No. 9357, http://www.ftc.gov/sites/default/files/documents/cases/140117labmdorder.pdf.
[50] *Id.* (citing Am. Fin. Servs. Ass'n v. FTC, 767 F.2d 957, 966 (D.C. Cir. 1985),
[51] *Id.*
[52] *Id.* (citing FTC v. Neovi, Inc., 604 F.3d 1150, 1155 (9th Cir. 2010) (creating and delivering unverified checks that enabled fraudsters to take unauthorized withdrawals from consumers' bank accounts); FTC v. Accusearch, Inc., 570 F.3d 1187, 1193 (10th Cir. 2009) (covert retrieval and sale of consumers' telephone billing information); Orkin Exterminating Co. v. FTC, 849 F.2d 1354, 1364 (11th Cir.1988) (unilateral breach of standardized service contracts); Am. Fin. Servs. Ass'n, 767 F.2d at 971 (oppressive litigation conduct to repossess household goods sold on credit).
[53] Philip Morris, Inc., 82 F.T.C. 16 (1973) (respondent had distributed free-sample razor blades in such a way that they could come into the hands of small children) (consent agreement).
[54] Holland Furnace Co. v. FTC, 295 F.2d 302 (7th Cir. 1961) (seller's servicemen dismantled home furnaces and then refused to reassemble them until the consumers had agreed to buy services or replacement parts).
[55] Orkin Exterminating Co., INC. v. F.T.C., NO. 87-8285, 849 F.2d 1354 (1988).
[56] FTC File No. 872-3193. FTC Docket No. 9236; FTC Charges Fitness Quest, Inc. with Making Deceptive Claims and Failing to Disclose a Safety Risk from Use of Its "Gut Buster" Exercise Device, http://www.casewatch.org/ftc/news/1990/gutbust.shtml ("Breakage has allegedly caused substantial physical injury to consumers, and failure to disclose such a risk is alleged to be an unfair practice.").

practices."[57] Many of the alleged unfair actions seek to take advantage of vulnerable consumers, making exploitation the locus of many unfairness allegations.[58]

Thus, Congress gave the FTC very broad and general regulatory authority by design to allow for a more nimble and evolutionary approach to the regulation of consumer protection.

2. Overlapping Domains

To what extent is the FTC's enforcement authority limited when it overlaps with other laws and regulations? Critics charge that the FTC cannot intrude upon the regulatory space of other agencies and that it cannot use Section 5 when there are more specific statutes dealing with a particular issue. This argument, however, is not consistent with how the FTC has operated for nearly a century. Moreover, if the FTC's Section 5 power were to stop at any overlapping regulatory domain, the result would be a confusing, contentious, and unworkable regulatory system with boundaries constantly in dispute.

In the early days of FTC data protection enforcement, the possibility of overlap was diminished because there were many fewer laws regulating data protection issues. The Fair Credit Reporting Act (FCRA) of 1970 already gave the FTC the authority to regulate the credit reporting industry. New data protection laws and regulation began to emerge after the FTC started applying Section 5 to data protection in the mid-1990s. For example, the Health Insurance Portability and Accountability Act (HIPAA) went into effect in 2003. The HITECH Act of 2009 added a data breach notification requirement to HIPAA.[59] In many circumstances, the FTC did not encroach upon existing enforcement authority of other agencies; these agencies acquired enforcement authority after the FTC had already been enforcing. It is important to note that when Congress passed HIPAA and later on when it passed the HITECH Act amending HIPAA, it did not include any provision restricting the FTC from enforcing against HIPAA-regulated entities. This omission is particularly salient for the HITECH Act of 2009, where many of the amendments to HIPAA involved provisions increasing HHS's enforcement powers and penalties, as well as the scope of HHS's enforcement (such as authorizing HHS to enforce against most entities that receive HIPAA-regulated data from a healthcare provider or other "covered entity" under HIPAA).

Although several laws gave the FTC additional enforcement powers, these powers were extensions beyond Section 5. For example, the Children's Online Privacy Protection Act (COPPA) of 1998 gave the FTC direct authority to enforce the statute's mandates for websites directed to children under 13. Under COPPA, the FTC was also granted rulemaking authority, which it lacked for the most part under Section 5. The Gramm-Leach-Bliley Act (GLBA) of 1999 gave the FTC direct authority over data protection in

---

[57] Stephen Calkins, FTC Unfairness: An Essay, 46 Wayne L. Rev. 1935, 1962 (2000).

[58] *See, e.g.*, R.F. Keppel & Bro., Inc v. FTC, 291 U.S. 304 at 313, 545 S.Ct. 423, 78 L.Ed. 814 (1934) (finding unfairness where an action ""exploits consumers, children, who are unable to protect themselves….:); Statement of Basis and Purpose of Trade Regulation Rule 408, Unfair or Deceptive Advertising and Labeling of Cigarettes in Relation to the Health Hazards of Smoking, 29 Fed. Reg. 8355 (1964) (quoted in Sperry and Hutchinson, supra at 244, n.5).

[59] *See* Health Information Privacy: HITECH Act Enforcement Interim Final Rule, U.S. Dep't of Health & Human Servs., http://www.hhs.gov/ocr/privacy/hipaa/administrative/enforcementrule/hitechenforcementifr.html.

the financial services industry. Previously, many entities in this industry (such as banks) were explicitly excluded from the FTC's Section 5 authority. Under GLBA, Congress gave the FTC rulemaking powers. Thus, Congress did not pass these data protection laws to give the FTC powers that it might have had under Section 5. Rather, it gave the FTC powers that augmented and extended what it was doing under Section 5. Had Congress thought that the FTC was overreaching in its early Section 5 enforcement, the passage of these statutes would have been a logical time to reign in the FTC to these specific domains. Instead, Congress did the opposite, and the result of these laws was to give the FTC a greater foothold in the field of data protection.

Given the breadth of Section 5 and its applicability to nearly every industry, as well as the rise of new privacy legislation, some overlap naturally developed. Does the FTC lose its power to regulate in these newly colonized areas? Does FTC regulation present problems of regulatory redundancy and inconsistency? What is the proper scope of FTC power in an area of overlap?

The most prominent argument that the FTC loses regulatory authority in an area of overlap is Wyndham's contention regarding the FTC's authority over data security. As discussed above, Wyndham claims that because Congress granted specific data security powers to the FTC in the GLBA and COPPA and because other statutes regulate data security (such as FCRA), this is a clear indication that the FTC lacks general authority to regulate data security.

However, there is simply no textual support for the categorical exclusion of data security, or for that matter *any* single class of actions absent a specific abdication of responsibilities with a cooperating/overlapping agency. Congress has yet to act in any explicit way to repeal the FTC's authority over data security. To the contrary, when Congress has enacted laws that involve data security, such as GLBA and COPPA, Congress has augmented the FTC's powers by adding data security rulemaking authority.

The FTC was created to have intentionally general and expansive jurisdiction. Instead of listing every area that the FTC's jurisdiction covers, the FTC Act specifically lists the areas it does not cover, including banks, savings and loan institutions, Federal credit unions, common carriers, air carriers, meat packers, and non-profit entities.[60] In its order denying LabMD's motion to dismiss, the Commission stated, "the FTC Act makes clear that, when Congress wants to exempt a particular category of entities or activities from the Commission's authority, it knows how to do so explicitly."[61] Section 5(a)(2) of the FTC Act contains a list of carve-outs where FTC jurisdiction does not apply, and Congress did not amend that list when it passed HIPAA or other data protection laws.[62]

Section 5's inevitable overlap with other statutes and regulatory domains is necessary and manageable. The FTC routinely shares regulatory authority with other administrative agencies. With respect to FTC overlapping and concurring jurisdiction, one court has stated, "Because we live in 'an age of overlapping and concurring regulatory

[60] 15 U.S.C. §45(a)(1)-(2). Non-profit entities are ostensibly not engaged in "commerce."
[61] Order Denying Respondent LabMD's Motion to Dismiss, In the Matter of LabMD, No. 9357, http://www.ftc.gov/sites/default/files/documents/cases/140117labmdorder.pdf (citing 15 U.S.C. § 45(a)(2)).
[62] Order Denying Respondent LabMD's Motion to Dismiss, In the Matter of LabMD, No. 9357, http://www.ftc.gov/sites/default/files/documents/cases/140117labmdorder.pdf (citing 15 U.S.C. § 45(a)(2)).

jurisdiction,' a court must proceed with the utmost caution before concluding that one agency may not regulate merely because another may.'"[63] Indeed, concurring and overlapping jurisdiction between administrative agencies and between agencies and statutes is not only common, but often desirable.[64] Jacob Gersen has argued, "A statute that allocates authority to multiple government entities relies on competing agents as a mechanism for managing agency problems. Giving authority to multiple agencies and allowing them to compete against each other can bring policy closer to the preferences of Congress than would delegation to a single agent."[65]

For example, the FTC has worked with the Food and Drug Administration (FDA) for over forty years regarding certain kinds of advertising for food and drugs.[66] Consumer protection is involved in so many different other domains because the range of commerce is so vast. Many different statutes and administrative agencies inevitably overlap with the FTC's potential reach, yet courts have explicitly found this overlap not to curtail the FTC's jurisdiction. For example, in examining FTC's deceptive advertising overlap with the Commodities Exchange Act (CEA) and Investment Advisors Act (IAA), one court stated "The proscriptions of the IAA are not diminished or confused merely because investment advisers must also avoid that which the FTC Act proscribes. And, because these statutes are 'capable of co-existence,' it becomes the duty of this court "to regard each as effective" – at least absent clear congressional intent to the contrary."[67]

The FTC has regularly "double dipped" when it considered activity in violation of both a statute over which the FTC has jurisdiction and Section 5. For example, almost half of the FTC complaints alleging violations of COPPA also contained an allegation of deceptive trade practices.[68] Almost all of the FTC complaints alleging violations of the

---

[63] FTC v Ken Roberts Co., 276 F3d 583, 593 (DC Cir 2001), quoting Thompson Medical Co. v FTC, 791 F2d 189, 192 (DC Cir 1986). See also FTC v Texaco, Inc., 555 F2d 862, 881 (DC Cir 1976). See generally FTC v Cement Institute, 333 US 683, 694-95 (1948).

[64] Jacob E. Gersen, Overlapping and Underlapping Jurisdiction in Administrative Law, 2006 Sup. Ct. Rev. 201, 208 (2006) ("statutes that parcel out authority or jurisdiction to multiple agencies may be the norm, rather than an exception." and "Because overlapping and underlapping jurisdictional assignment can produce desirable incentives for administrative agencies, statutes [that create overlapping and underlapping jurisdictional schemes] are useful tools for managing principal-agent problems inherent in delegation.").

[65] Jacob E. Gersen, Overlapping and Underlapping Jurisdiction in Administrative Law, 2006 Sup. Ct. Rev. 201, 212 (2006).

[66] *See* Memorandum of Understanding Between The Federal Trade Commission and The Food and Drug Administration, MOU 225-71-8003, http://www.fda.gov/AboutFDA/PartnershipsCollaborations/MemorandaofUnderstandingMOUs/DomesticMOUs/ucm115791.htm; THOMPSON MEDICAL CO., INC. V. FEDERAL TRADE COMMISSION, 1986 WL 1275690, 791 F2d 189, 192 ("We find no evidence in the regulatory scheme that Congress has fashioned for over-the-counter medications that the FTC is indefinitely barred from all regulatory authority over drug advertising while the FDA conducts its comprehensive review of drug safety. Nowhere in the case law or in the FTC's grant of authority is there even a hint that the FTC's jurisdiction is so constricted. To the contrary, the cases recognize that ours is an age of overlapping and concurring regulatory jurisdiction."); *see also* Overlapping Authority of FTC, CCH-DCLR P 2010.85 (C.C.H.), 2009 WL 5076333 ("The Federal Trade Commission has jurisdiction to prohibit false labeling and misbranding of food, drugs and cosmetics and other products where the false labeling and misbranding constitutes unfair competition in the purview of Section 5 of the FTC Act") (citing Fresh Grown Preserve Corp. v. FTC(2d Cir. 1942) 125 F2d 917).

[67] F.T.C. v. Ken Roberts Co., 276 F.3d 583, 593 (D.C. Cir. 2001).

[68] United States v. Artist Arena, Complaint, FTC File No. 112 3167, http://www.ftc.gov/os/caselist/1123167/121003artistarenacmpt.pdf (2012); United States v. Rock You, Complaint, FTC File No. 1023120, http://www.ftc.gov/os/caselist/1023120/120327rockyoucmpt.pdf (2012); United States v. Godwin, Complaint, FTC File No. 1123033, http://www.ftc.gov/os/caselist/1123033/111108skidekidscmpt.pdf (2011); United States v. Playdom,

GLBA also contained an allegation of deceptive or unfair trade practices.[69] These practices have not resulted thus far in any Congressional backlash. Congress has had ample time to curtail clear instances of overlap but has not done so. As we noted earlier, the most significant example is with the HITECH Act of 2009 where Congress directly addressed HHS's enforcement power and could have limited that power exclusively to HHS. Interestingly, Congress chose to allow for more entities to enforce by authorizing state attorneys general to enforce HIPAA.

Although there is overlap, it has not resulted in significant inconsistencies or confusion. The FTC and HHS often coordinate enforcement actions for violations that implicate both HIPAA and the FTC Act."[70] Moreover, as we noted in a previous work, the data

---

Complaint, FTC File No. 1023036, http://www.ftc.gov/os/caselist/1023036/110512playdomcmpt.pdf (2011); United States v. Iconix, Complaint, FTC File No. 0923032, http://www.ftc.gov/os/caselist/0923032/091020Iconixcompletecmpt.pdf (2009); In re Sony BMG, Complaint, FTC File No. 062-3019, http://www.ftc.gov/os/caselist/0623019/0623019cmp070629.pdf (2007); United States v. American Pop Corn Company, Complaint, FTC File No. 012 3026), http://www.ftc.gov/os/2002/02/popcorncmpnt.pdf (2002); United States v. Lisa Frank, Complaint, FTC File No. 012-3050, http://www.ftc.gov/os/2001/10/lfcmp.pdf (2001); United States v. Bigmailbox.com, Complaint, File No. 002 3378, http://www.ftc.gov/os/2001/04/bigmailboxcmp.pdf (2001); FTC v. Toysmart, First Amended Complaint for Permanent Injunction and Other Equitable Relief, File No. X000075, http://www.ftc.gov/os/2000/07/toysmartcomplaint.htm (2000); United States v. Path, Complaint, FTC File No. 122 3158, http://www.ftc.gov/os/caselist/1223158/130201pathinccmpt.pdf (2013). It is not always clear if the FTC is alleging a violation of COPPA, a violation of Section 5, or both. For example, in *W3 Innovations*, the FTC initially alleges that a violation of the COPPA rule constitutes an unfair or deceptive trade practice, yet only appears to bring one count of violating the COPPA rule against the defendant. United States v. W3 Innovations, Complaint, FTC File No. 102 3251, http://ftc.gov/os/caselist/1023251/110815w3cmpt.pdf (2011); United States v. Industrious Kid, Complaint, FTC File No.: 072-3082, http://www.ftc.gov/os/caselist/0723082/080730comp.pdf (2008); United States v. Xanga, Complaint, FTC File No. 062-3073, http://www.ftc.gov/os/caselist/0623073/060907xangacomplaint.pdf (2006) (alleging that "Pursuant to Section 18(d)(3) of the FTC Act, 15 U.S.C. § 57a(d)(3), a violation of the [COPPA] Rule constitutes an unfair or deceptive act or practice."). Contrast this with other FTC complains where both the COPPA rule and Section 5 were alleged to have been violated). *See, e.g.*, United States v. Playdom, Complaint, FTC File No. 1023036, http://www.ftc.gov/os/caselist/1023036/110512playdomcmpt.pdf (2011) (alleging violations of COPPA and a separate Section 5 of the FTC Act independent of a COPPA violation).

[69] In re Franklin's Budget Car Sales, Complaint, FTC File No. 102 3094, http://www.ftc.gov/os/caselist/1023094/121026franklinautomallcmpt.pdf (2012); In re Premier Capital Lending, Complaint, FTC File No. 0723004, http://www.ftc.gov/os/caselist/0723004/081206pclcmpt.pdf (2008); In re Goal Financial, Complaint, FTC File No. 072-3013, http://www.ftc.gov/os/caselist/0723013/080415complaint.pdf (2008); In re Superior Mortgage, Complaint, File No. 052 3136, http://www.ftc.gov/os/caselist/0523136/051216comp0523136.pdf (2005; FTC v. Sun Spectrum Communications, Complaint, FTC File No. 032 3032, http://www.ftc.gov/os/caselist/0323032/031202cmp0323032.pdf (2004).; United States v. Global Mortgage Funding, Complaint, FTC File No.: 062 3107, http://www.ftc.gov/os/caselist/0623107/071030globalmtgfundingcmplt.pdf (2007); FTC v. Corporate Marketing Solutions, Complaint, FTC File No. 022-3001, http://www.ftc.gov/os/2002/07/cmscmp.pdf (2002); FTC v. Guzzetta, Complaint, File No. 012 3066, http://www.ftc.gov/os/2001/04/pretextingsmartdatacomplaint.pdf (2001); FTC v. Garrett, Complaint, FTC File No.:012 3067, http://ftc.gov/os/2002/03/discreetdatacmplnt.pdf (2002); In re Nations Title Agency, Complaint, File No. 052 3117, http://www.ftc.gov/os/caselist/0523117/0523117NationsTitle_Complaint.pdf (2006).

[70] Order Denying Respondent LabMD's Motion to Dismiss, In the Matter of LabMD, No. 9357, http://www.ftc.gov/sites/default/files/documents/cases/140117labmdorder.pdf (citing HHS, Modifications to the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules, Final Rule, 78 Fed. Reg. 5566, 5579 (Jan. 25, 2013)).

security standards that the FTC has developed are quite consistent with those in the HIPAA Security Rule.[71]

The FTC's jurisprudence overlaps substantially with torts and contracts as well. For example, the tort law analog to deception under Section 5 is the tort of fraud. The FTC's enforcement of promises made in privacy policies in many ways overlaps the law of contract and promissory estoppel.[72]

Thus, the FTC's data protection authority is not a unique case of overlap, but one example among many instances of overlap that understandably arise given the breadth of the FTC's Section 5 authority. Moreover, given the absence of a federal omnibus data protection statute, the basic United States approach to data protection is to have a series of different laws to regulate different corners of the economy. Modern industry is complex and does not follow neatly-designed regulatory boundaries, especially when these laws are passed over the course of decades. Today, companies dance nimbly between different economic sectors. A technology company can enter the healthcare domain, and can have components that fall into financial services and other arenas. Regulatory overlap is bound to happen as industries shift to evolve with a rapidly-changing economy.

More broadly, a rigid prohibition on regulatory overlap would prove quite challenging and chaotic. Agencies would clash in carving out contiguous borders when their regulatory scopes overlap. And these borders would have to be adjusted with each new law that creates potential overlap.[73] In sum, the idea that potential regulatory overlap disqualifies the FTC from regulating data security is not supported in theory or in practice. The FTC regularly manages its concurring and overlapping jurisdiction in ways that allow it to fill gaps as well as refine its theories of regulation.

3. Adequate Notice and the Gradual Development of Rules

Critics of the FTC's approach to data protection have claimed that the FTC has failed to provide proper notice in advance of what companies must do to avoid liability.[74] They contend that the FTC simply waits until after a data breach occurs and then announces

---

[71] Daniel J. Solove and Woodrow Hartzog, The FTC and the New Common Law of Privacy, 114 Colum. L. Rev. 583 (2014),http://ssrn.com/abstract=2312913.

[72] Daniel J. Solove and Woodrow Hartzog, The FTC and the New Common Law of Privacy 583 (2014), http://papers.ssrn.com/sol3/papers.cfm? abstract_id=2312913.

[73] *See generally* Jacob E. Gersen, Overlapping and Underlapping Jurisdiction in Administrative Law, 2006 Sup. Ct. Rev. 201, 208 (2006).

[74] Motion to Dismiss by Wyndham Hotels & Resorts LLS, FTC v. Wyndham Worldwide Corp., No. 2:12-cv-01365-SPL (D. Ariz. filed Aug. 27, 2012); Respondend LabMD's Motion to Dismiss Complaint with Prejudice and to Stay Administrative Proceedings, In the Matter of LabMD, Docket No. 9357 (on file with authors); Amici Curiae Brief of TechFreedom, International Center for Law and Economics & Consumer Protection Scholars, FTC v. Wyndham Worldwide Corp. No. 2:12-cv-01365-SPL (D. Ariz. filed June 17, 2013), http://docs.techfreedom.org/Wyndham_Amici_Brief.pdf; Gerard M. Stegmaier and Wendell Bartnick, Psychics, Russian Roulette, and Data Security: The Ftc's Hidden Data-Security Requirements, 20 Geo. Mason L. Rev. 673 (2013); Gerard M. Stegmaier and Wendell Bartnick, Another Round in the Chamber: Ftc Data Security Requirements and the Fair Notice Doctrine, 17 J. Internet L. 1 (2013); Michael D. Scott, The FTC, the Unfairness Doctrine, and Data Security Breach Litigation: Has the Commission Gone Too Far?, 60 Admin. L. Rev. 127 (2008); Brief of Amici Curiae Chamber of Commerce of the United States of America, Retail Litigation Center, and American Hotel and & Lodging Association in Support of Defendants, FTC v. Wyndham Worldwide Corp., Case No. CV 12-1365-PHX-PGR..

new data security rules and standards that the companies suffering the breach should have followed.[75] This practice, the critics charge, fails to provide companies with sufficient advance warning about what is required in order to provide acceptable data security.

Companies like LabMD and Wyndham have also argued that the FTC should have to create rules after a formal process, rather than rely on creating rules case-by-case, which the companies claim fails to give the requisite amount of notice. LabMD argued in its motion to dismiss that "the FTC admits that it has not prescribed regulations or legislative rules under Section 5 establishing patient-information (or any other) data-security standards that have the force of law. The FTC's refusal to issue regulations is wrongful and makes no sense."[76] Wyndham stated in support of its argument that it lacked fair notice that "if the FTC can regulate data security at all, it must do so through published rules that give regulated parties fair notice of what the law requires."[77] An implication of this argument is that the FTC is engaging in a kind of rulemaking through its cases, and making rules is beyond its powers in this area since the FTC lacks specialized rulemaking authority under Section 5.[78] Moreover, another implication of this argument is that rules are better when created according to a formal rulemaking process, where stakeholders can submit comments, where rules can be worked out more systematically, and where there is greater notice.

However, this argument and entire line of reasoning misunderstands firmly established reasonableness approaches that obligate companies to reasonably follow industry standards. Many critics seem to want a "check list" of data security practices that will, in essence, provide a safe harbor in all contexts. Yet data security changes too quickly and is far too dependent upon context to be reduced to a one-size-fits-all checklist.[79] Instead, the FTC has opted to defer to industry to set the appropriate standards for good data security practices by utilizing a "reasonableness" standard.

---

[75] Motion to Dismiss by Wyndham Hotels & Resorts LLS, FTC v. Wyndham Worldwide Corp., No. 2:12-cv-01365-SPL (D. Ariz. filed Aug. 27, 2012) at. 6-7.

[76] Respondent LabMD's Motion to Dismiss Complaint with Prejudice and to Stay Administrative Proceedings, In the Matter of LabMD, Docket No. 9357 (on file with authors) at 23-24.

[77] Reply in Support of Motion to Dismiss by Wyndham Hotels & Resorts LLC, FTC v. Wyndham Worldwide Corp., Case No. CV 12-1365-PHX-PGR at 7.

[78] The FTC has only Magnuson-Moss rulemaking authority, which is so procedurally burdensome that it is largely ineffective. Beth DeSimone and Amy Mudge articulate why the Magnuson-Moss rules are largely ineffective:

> Right now, the FTC is constrained in its rulemaking by the so-called "Magnuson-Moss" rules. These rules require the FTC Staff to engage in an industry-wide investigation, prepare draft staff reports, propose a rule, and engage in a series of public hearings, including cross-examination opportunities prior to issuing a final rule in any area. These processes are so burdensome that the FTC has not engaged in a Magnuson-Moss rule-making in 32 years.

Beth DeSimone & Amy Mudge, Is Congress Putting the FTC on Steroids?, Seller Beware Blog, Arnold & Porter (Apr. 26, 2010), http://www.consumeradvertisinglawblog.com/2010/04/is-congress-putting-the-ftc-on-steroids.html; see also FTC, Operating Manual ch. 7, available at http://www.ftc.gov/foia/ch07rulemaking.pdf.

[79] *See, e.g.*, Framework for Improving Critical Infrastructure Cybersecurity, National Institute of Standards and Technology (Feb. 12, 2014), http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214-final.pdf ("Organizations may choose to handle risk in different ways, including mitigating the risk, transferring the risk, avoiding the risk, or accepting the risk, depending on the potential impact to the delivery of critical services….The Framework is adaptive to provide a flexible and risk-based implementation that can be used with a broad array of cybersecurity risk management processes.").

A "reasonableness" standard is already one the most established and proven touchstones for regulating data security. For example, Maryland requires that "a business that owns or licenses personal information of an individual residing in the State shall implement and maintain reasonable security procedures and practices that are appropriate to the nature of the personal information owned or licensed and the nature and size of the business and its operations."[80] In California, "[a] business that owns or licenses personal information about a California resident [must] implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use, modification, or disclosure."[81] There are a number of other states that also require "reasonable" data security practices.[82] The Fair Credit Reporting Act requires that certain employers properly dispose of customer information by taking "reasonable measures" to protect against the unauthorized access and possession of the information.[83] Under HIPAA, holders of protected health identifiers must use "reasonable and appropriate" means to ensure that administrative, physical and technical safeguards are in place to protect data and control access to it and that risk assessments conducted and security policies and procedures are documented.[84]

Reasonableness standards permeate many traditional legal concepts. The entire tort of negligence is largely a "duty to act reasonably under the circumstances" and many contractual obligations are also hitched to reasonableness. Indeed, this fact was explicitly acknowledged by Commissioner Josh Wright, writing for a unanimous Commission in denying LabMD's motion to dismiss:

---

[80] The Personal Information Protection Act (PIPA), Md. Code Ann., Com. Law § 14-3503 (West).

[81] Cal. Civ. Code § 1798.81.5 (West Supp. 2008).

[82] Ark. Code Ann. § 4-110-104(b) (Supp. 2007) ("A person or business that acquires, owns, or licenses personal information about an Arkansas resident shall implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information from unauthorized access, destruction, use, modification, or disclosure"); 2008 Conn. Acts No. 08-167 (Reg. Sess.) ("Any person who conducts business in the state and maintains personal information shall implement and maintain reasonable procedures to: (a) prevent unlawful use or disclosure of personal information collected or maintained in the regular course of business"); Nev. Rev. Stat. Ann. § 603A.210 (West Supp. 2007) ("data collector that maintains records which contain personal information of a resident of this State shall implement and maintain reasonable security measures to protect those records from unauthorized access, acquisition, destruction, use, modification or disclosure"); N.C. Gen. Stat. § 75-64(a) (2007) (defining obligated reasonable measures to include "Implementing and monitoring compliance with policies and procedures that require the burning, pulverizing, or shredding of papers containing personal information so that information cannot be practicably read or reconstructed.(2) Implementing and monitoring compliance with policies and procedures that require the destruction or erasure of electronic media and other nonpaper media containing personal information so that the information cannot practicably be read or reconstructed.(3) Describing procedures relating to the adequate destruction or proper disposal of personal records as official policy in the writings of the business entity."); Or. Rev. Stat. Ann. § 646A.622(1) (West Supp. 2008) ("Any person that owns, maintains or otherwise possesses data that includes a consumer's personal information that is used in the course of the person's business, vocation, occupation or volunteer activities must develop, implement and maintain reasonable safeguards to protect the security, confidentiality and integrity of the personal information, including disposal of the data" and explicitly recognizing compliance with GLB or HIPAA data security standards as "reasonable."); R.I. Gen. Laws § 11-49.2-2(2) (Supp. 2007) ("A business that owns or licenses computerized unencrypted[sic] personal information about a Rhode Island resident shall implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use, modification, or disclosure."); Utah Code Ann. § 13-44-201(1)(a) (Supp. 2007) ("Any person who conducts business in the state and maintains personal information shall implement and maintain reasonable procedures to: (a) prevent unlawful use or disclosure of personal information collected or maintained in the regular course of business.").

[83] 16 C.F.R. § 682.3(a) (2007).

[84] 45 C.F.R. §§ 164.308-.314.

> LabMD's due process claim is particularly untenable when viewed against the backdrop of the common law of negligence. Every day, courts and juries subject companies to tort liability for violating uncodified standards of care, and the contexts in which they make those fact-specific judgments are as varied and fast-changing as the world of commerce and technology itself.[85]

As Commissioner Wright noted, tort liability can be as unpredictable as FTC enforcement, and torts can involve "compensatory and even punitive damages." Despite these facts, "it is well-established that the common law of negligence does not violate due process simply because the standards of care are uncodified."[86]

Reasonableness is also the locus for Fourth Amendment analysis of searches.[87] Of course, for certain circumstances, a set of rules can be a more effective regulatory tool. In the debate between rules and standards, between more systematic and case-by-case legal development, there is no universal winner. The U.S. system of law consists of a mix of these approaches.

In a common law system – or any system where matters are decided case-by-case and there is an attempt at maintaining consistency across decisions, any reasonableness standard will evolve into something more akin to a rule with specifics over time. Indeed, any broad standard will follow this evolutionary trajectory. Such a developmental pattern is inevitable if prior decisions have any kind of precedential effect or the functional equivalent of precedent. The standard will start out rather broadly, but each new case will bring a new application of that standard to a concrete situation. From these collected specific applications, the details start to accumulate around the standard's skeletal frame. Each case typically fills in something. Of course, if these decisions did not have any effect on future decisions, then the standard would remain in its pristine skeletal state. But in the U.S. system of law, prior cases, including interpretations and applications of statutes and regulations, are not ignored. In contrast to civil law systems, in common law systems such as the U.S., there is an overarching and very powerful norm for consistency across decisions and to avoid deviating from prior decisions.

While some initial uncertainty might be the present at the outset, the clarity provided by each additional legal action virtually guarantees ever increasing determinism for those already charged with a reasonable adherence to commonly shared industry standards.

The FTC is not exceeding its authority because this developmental pattern is practically inevitable and quite predictable given the clarity offered by incorporation of generally accepted industry practices and the wiggle room provided by requiring reasonable but not strict adherence to those practices.

---

[85] Order Denying Respondent LabMD's Motion to Dismiss, In the Matter of LabMD, Inc., FTC.gov, http://www.ftc.gov/sites/default/files/documents/cases/140117labmdorder.pdf.
[86] *Id.*
[87] Jeffrey Bellin, Crime-Severity Distinctions and the Fourth Amendment: Reassessing Reasonableness in A Changing World, 97 Iowa L. Rev. 1, 8 (2011) ("The Court's opinions emphasize that the "touchstone of the Fourth Amendment is reasonableness").

Thus, standards evolve in a developmental pattern typical of the common law and the product of adherence to precedent, consistency in decisions, and case-by-case adjudication over time. If this pattern were not present, then the FTC would be acting inconsistently, ignoring previous actions, or reaching too far beyond particular cases. In fact, the FTC has been quite clear and consistent in its approach. It has not developed theories that are at odds with previous complaints, nor does it dramatically lurch in dramatic, unpredictable or haphazard ways.

With or without rulemaking authority, it is inevitable that the FTC will be developing rules. This is just the byproduct of the FTC enforcing broad standards, memorializing how it is interpreting those standards in particular cases, and being consistent with its prior interpretations. The FTC has not been engaging in rulemaking in disguise any more than a court when interpreting a statute over time is engaging in judicial legislation. This is just a common law styled system at work, and the norms and practices of this system, such as adherence to precedent, apply to statutory and constitutional interpretation as well.

The court in *Wyndham* affirmed the FTC's case-by-case approach in the face of a fair notice challenge, noting that "Circuit Courts of Appeal have affirmed FTC unfairness actions in a variety of contexts *without* preexisting rules or regulations specifically addressing the conduct-at-issue."[88] Although the court agreed that laws must give fair notice of conduct that is forbidden or required, it was not convinced that regulations are the only means of providing sufficient fair notice. Judge Salas seemed to understand that the rapidly evolving nature of data security made the FTC's analogies to the NLRB and OSHA as models of bringing enforcement actions without issuing particularized prohibitions persuasive.

Perhaps more importantly, the court noted that "the contour of an unfairness claim in the data-security context, like any other, is necessarily 'flexible' such that the FTC can apply Section 5 'to the facts of particular cases arising out of unprecedented situations.'"[89] The court validated a reasonableness approach built upon industry standards and shaped by administrative actions. The court quoted *General Electric Co. v. Gilbert*,[90] which declared that "the rulings, interpretations and opinions of the Administrator under this Act, while not controlling upon the courts by reason of their authority, do constitute a body of experience and informed judgment *to which courts and litigants may properly resort for guidance*."[91]

The court stated that Wyndham's argument regarding the intolerable vagueness of Section 5 unfairness "ignores that, in addition to various sources of guidance for measuring reasonableness, a statutorily-defined standard exists for asserting an unfairness claim."[92] The court also noted the illogical and unacceptable practical consequences of a mandate for specific rules before bringing a complaint, stating "the FTC would have to cease brining *all* unfairness actions without first proscribing particularized prohibitions—

[88] *Id.* (citing FTC v. Neovi, Inc., 604 F.3d 1150, 1153, 1155-59 (9th Cir. 2010); FTC v. Accusearch Inc., 570 F.3d 1187, 1191, 1193-95 (10th Cir. 2009)).
[89] *Id.* at 23 (citing FTC v. Colgate-Palmolive Co. 38 U.S. 374, 384-85 (1965)).
[90] 429 U.S. 125, 141-42 (1976).
[91] *Id.* (emphasis added in FTC v. Wyndham Worldwide Corp., No. 13-1887 Slip Op. (April 7, 2014 D.N.J.) at 24).
[92] FTC v. Wyndham Worldwide Corp., No. 13-1887 Slip Op. (April 7, 2014 D.N.J.) at 25.

a result that is in direct contradiction with the flexibility necessarily inherent in Section 5 of the FTC Act."[93]

Our previous research demonstrates the validity of the court's conclusion that the FTC's interpretations of the FTC Act provide sufficient guidance.[94] For example, at the time we wrote the article, there were over 40 FTC complaints and consent decrees regarding data security and we reviewed all of them. When reviewed in their totality, far from being vague and arbitrary, we were able to compile a list of specific security practices that the FTC has deemed as inadequate.[95] Moreover, most of these bad practices are ones that clearly run afoul of industry standards or other regulation. Like the data security requirements of HIPAA and GLB, the FTC has given notice through its that failure to have reasonable physical, technical, and administrative safeguards constitutes an unfair trade practice.

Some critics demand that the only detailed rules would provide the kind of guidance industry needs to protect personal data, but centuries of common law development prove otherwise. The common law has achieved a sufficient specificity, predictability, and clarity that can rival that of statutes.

A common law style of rule development has certain benefits. There is flexibility to adapt to new situations. The FTC can wait until a consensus around standards develops and then codify them as this happens. With data protection, the norms and standards have been developing significantly over the past few decades, and there has not been consensus around a complete rule set. Rather than wait decades for such a consensus to develop, the FTC has been able to engage in the functional equivalent of codifying those rules and standards that have achieved sufficient consensus. The common law style recognizes that Rome was not built in a day; and that one need not have a complete blueprint to begin building.

II. DEFINING THE FTC'S ROLE IN DATA PROTECTION

Thus far, we have argued that the FTC has broad data protection enforcement power, and that the critics are wrong in the constraints they propose on this power. In this Part, we move beyond descriptive claims about the scope of FTC data protection power to the normative issues. Should the FTC have such broad powers in this area? Is the FTC being too aggressive in regulating data protection? Should it pull back? Or should it expand its foothold in this area?

We contend that the FTC not only should have broad data protection enforcement powers, but that it also should be exercising these powers more robustly. The FTC should enforce more expansively, embrace consensus norms more quickly, and take more of a leadership role in the development of privacy norms and standards.

---

[93] *Id.*
[94] Daniel J. Solove and Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, 114 COLUM. L. REV. 583 (2014), available at http://ssrn.com/abstract=2312913.
[95] *Id.* at 651-55.

The FTC has established a foundation for being the U.S. data protection authority. We argue that the FTC should build aggressively on this foundation to more fully take on this role.

For the most part, the FTC has been quite conservative in its data protection enforcement. The FTC has been more of a norm-codifier than a norm-maker. Thus far, the FTC has developed its jurisprudence in a measured and modest way. It is time for the FTC to become less conservative in its approach. Rapid technological change continues to vex courts and lawmakers or leave consumers vulnerable to privacy harms. U.S. privacy law is a chaotic jumble of different laws, with gaps and inconsistencies, and the U.S. approach is at odds with most other countries in the world, which have broader and more omnibus privacy laws. A broad privacy law spanning most industries would be politically impractical given the way Congress is structured as well as the current stalemate in Congress. There is little hope in Congress passing any privacy-related legislation anytime soon, as demonstrated by regularly unsuccessful legislative proposals.[96] The FTC is one of the best hopes for guiding U.S. privacy law to a more coherent and stable regulatory system.

A. Lynchpin of U.S. Data Protection Law

In the current U.S. privacy regulatory system, the FTC has grown into the role of being the leading regulator of privacy, a key lynchpin giving coherence to a partly self-regulatory system that has increasingly become regulated by a jumble of different data protection laws at the federal and state level. We contend that this role is critical to the system's legitimacy and ability to function.

In contrast to most other countries, the U.S. regulates privacy with a sectoral rather than omnibus approach. This means that there are a multitude of different laws regulating different industries rather than just one general statute to regulate all collection and use of personal data. In several instances, particular sectoral laws leave gaps where entire industries lack privacy regulation.[97] These industries can be regulated in certain dimensions by certain state laws or common law torts, but a large bulk of their activities can remain unregulated.

As the Internet matured in the 1990s, the gaps in the sectoral approach were quite significant. For example, the healthcare industry and much of the financial services industry lacked federal privacy regulation. These gaps eventually closed. But significant gaps remain. For example, there is no federal law that regulates much of online commerce. Merchants such as Amazon.com lack any federal sectoral law to regulate the

[96] *See* Tim Lisko, *112th Privacy Legislation*, PRIVACYWONK, http://www.privacywonk.net/2011/08/112th-privacy-legislation.php (last updated Feb. 7, 2012) (detailing federal legislation proposed in the 112th Congress); Craig Hoffman, *Online Privacy and Data Security Legislation Update – 2011 Year in Review*, DATA PRIVACY MONITOR (Dec. 28, 2011), http://www.dataprivacymonitor.com/federal-legislation/online-privacy-and-data-security-legislation-update-2011-year-in-review/; *EPIC Bill Track Tracking Privacy, Speech, and Cyber-Liberties Bills in the 111th Congress*, EPIC, http://epic.org/privacy/bill_track.html (last visited Jan. 31, 2014).

[97] *See, e.g.*, Lior Jacob Strahilevitz, Toward A Positive Theory of Privacy Law, 126 Harv. L. Rev. 2010, 2011-12 (2013) ("The sectoral U.S. approach, which lacks an effective catch-all provision, renders American law both reactive and slow to react. As a result, by the time U.S. regulators seek to challenge an envelope-pushing practice, interest groups supporting the practice have developed, social norms have adjusted to the practice, and a great deal of the sensitive information at issue has already been disclosed by consumers.").

privacy of personal data they collect and use when selling the majority of their products and services. Critics of the sectoral regime decried it.[98]

Concerned about consumer concerns and trust, online companies voluntarily made promises about data protection in privacy policies. Originally a feature of websites, privacy policies began to become common offline too, especially after the GLBA began requiring them for financial institutions and HIPAA began requiring them for healthcare institutions.

The making of promises in privacy policies was essentially a self-regulatory system. Companies could voluntarily decide whether to make a promise or not. The policies did not specify any sanctions if the promises were not kept. Moreover, hardly any attempts were made to enforce the privacy policies under contract law or promissory estoppel.[99] Data protection in many contexts merely amounted to promises backed up by nothing.
This system was viewed with scorn by many commentators, who found the privacy policies to be a hollow and toothless means of protecting privacy. Professors Edward Janger and Paul Schwartz noted the unhappiness felt by both privacy advocates and the financial sector over the self-regulatory system via privacy policies.[100] The Privacy Rights Clearinghouse stated that regarding the mandatory privacy notices under the GLB Act, "Industry, government agencies, and consumer education organizations . . . would all do well to view the year 2001 as a costly experiment that resulted in little effective education of the public about the rights to privacy of personal financial information under GLB."[101] Janger and Schwartz noted, "This conclusion has been echoed by Federal Trade Commission Chairman Timothy Muris, who summarized the net result of GLB privacy notices in these terms: 'Acres of trees died to produce a blizzard of barely comprehensible privacy notices.' It may, in fact, be a rare legislative feat to have a single statute create so many diverse critics so quickly."[102]

It was not clear that this self-regulatory system along with a few sectoral laws would last. The system was not even held together with chicken wire, and it was hard to view it as a coherent way to regulate data protection.

---

[98] *See, e.g.*, Joel R. Reidenberg, Privacy in the Information Economy: A Fortress or Frontier for Individual Rights?, 44 Fed. Comm. L.J. 195, 236 (1992) ("Since information processing occurs today throughout every industry, the privacy concerns are not unique to activities in any one context. Because privacy rights in the United States for commercial information processing depend on legislation targeted at narrow problems and rather limited common law rights, the lack of a coherent and systematic approach to existing privacy concerns presents an undesirable policy void."); Joel R. Reidenberg, E-Commerce and Trans-Atlantic Privacy, 38 Hous. L. Rev. 717, 725 (2001) ("American law is sporadic, confused, and wholly inadequate to protect citizens in the face of privacy-invasive technical advances and pervasive online commercial surveillance."); Kamaal Zaidi, Harmonizing U.S.-EU Online Privacy Laws: Toward A U.S. Comprehensive Regime for the Protection of Personal Data, 12 MICH. ST. J. INT'L L. 169, 172 (2003) ("A drawback to the sectoral approach is that it is difficult to develop and enforce uniform privacy standards when other industries not within the purview of government regulation have varying standards.").

[99] Daniel J. Solove and Woodrow Hartzog, The FTC and the New Common Law of Privacy (Aug. 19, 2013), available at http://papers.ssrn.com/sol3/papers.cfm? abstract_id=2312913

[100] Edward J. Janger & Paul M. Schwartz, The Gramm-Leach-Bliley Act, Information Privacy, and the Limits of Default Rules, 86 Minn. L. Rev. 1219, 1261 (2002) (citing Tena Friery & Beth Givens, 2001: The GLB Odyssey--We're Not There Yet, at http://www.privacyrights.org/ar/fp-glb-ftc.htm (Dec. 4, 2001)).

[101] Tena Friery & Beth Givens, 2001: The GLB Odyssey--We're Not There Yet, at http://www.privacyrights.org/ar/fp-glb-ftc.htm (Dec. 4, 2001).

[102] Edward J. Janger & Paul M. Schwartz, The Gramm-Leach-Bliley Act, Information Privacy, and the Limits of Default Rules, 86 Minn. L. Rev. 1219, 1261 (2002) (citing Timothy J. Muris, Protecting Consumers' Privacy: 2002 and Beyond, at http://www.ftc.gov/speeches/muris/privisp1002.htm (Oct. 4, 2001)).

The FTC stepped into this rather rickety patchwork of promises and narrow laws, and it used its broad Section 5 to fortify this regime. Initially, the FTC began enforcing promises made in privacy policies, giving the promises a stronger backbone.[103] 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.

The FTC currently remains a key lynchpin in the U.S. data protection regulatory regime. Its policing of privacy policies has matured into a more robust set of substantive requirements. Norms around best privacy and data security practices have developed. The FTC has increasingly looked to these norms to add flesh to the very broad concepts of deception and unfairness.

In case-by-case fashion, largely by consent decree, the FTC has developed a data protection jurisprudence that has many attributes of the common law.[104] 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 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.

Moreover, the FTC also 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.[105] The EU did not find US data protection law to be adequate in its protection of privacy, and the EU Data Protection Directive directs EU member nations to avoid transferring data to countries that lack an adequate level of protection. The US hammered out the Safe Harbor Arrangement with the EU where data could be transferred to companies that agreed to follow basic privacy principles and be subject to FTC enforcement. Once again, the FTC turned promises that would otherwise have been too soft into a more hardened form of protection.

Indeed, 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. The E.U. Safe Harbor is already on very shaky ground in light of the extent of US surveillance internationally.[106] Robert Gellman has noted this

[103] Daniel J. Solove and Woodrow Hartzog, The FTC and the New Common Law of Privacy (Aug. 19, 2013), available at http://papers.ssrn.com/sol3/papers.cfm? abstract_id=2312913.
[104] Daniel J. Solove and Woodrow Hartzog, The FTC and the New Common Law of Privacy (Aug. 19, 2013), available at http://papers.ssrn.com/sol3/papers.cfm? abstract_id=2312913.
[105] *See generally*, The EU-US Safe Harbor: An Analysis in the Framework's Effectiveness in Protecting Personal Privacy, The Future of Privacy Forum, http://www.futureofprivacy.org/wp-content/uploads/FPF-Safe-Harbor-Report.pdf.
[106] Jules Polonetsky, Dangerously Shortsighted: Keeping European Data in Europe, LinkedIn (Feb. 17, 2014), http://www.linkedin.com/today/post/article/20140217122658-258347-dangerously-shortsighted-keeping-european-data-in-europe; US-EU SAFE HARBOR UNDER PRESSURE, IAPP Privacy Tracker (Aug. 2, 2013), https://www.privacyassociation.org/privacy_tracker/post/us_eu_safe_harbor_under_pressure

instability as well, stating "Without the possibility of FTC enforcement, the entire Safe Harbor process would be in danger of collapse."[107]

B. Toward a More Expansive FTC Role in Data Protection

The FTC's role in data protection is not only legally and normatively justified, but it should also be expanded. Because the FTC is the only agency currently capable of responding to a number of vexing privacy issues, the agency can and should more aggressively use its power under Section 5 to develop a coherent U.S. system of data protection law.

1. An Emergent Data Protection Authority

A more centralized and comprehensive approach to data protection is sorely needed in the U.S., which is increasingly at odds with most other countries in the world in its more fragmented sectoral approach to data protection. The chances of Congress passing a comprehensive federal data protection law are remote. The most practical way that the U.S. data protection regime will evolve into something more coherent and comprehensive is through the FTC. Although it is unlikely the U.S. will ever have a European-style comprehensive data protection statute, the U.S. might be able to move closer to Europe and much of the rest of the world with a ground-up approach.

Of course, there will always be industries and contexts where different regulatory standards work better, so totally abandoning any sectoral differences is not desirable. But establishing some baseline standards and closing gaps are essential for the U.S. privacy regime to respond to existing and oncoming problems. More than any other agency, the FTC has the power and ability to lead the way, but to do so, it must become more aggressive in its activities.

In European Union countries, and in many other countries around the world, there is a central data protection authority. A "data protection authority" (DPA) is a governmental entity that is focused on regulating privacy and that does so across most industries.[108] In contrast, the United States lacks a DPA. Instead, various statutes and various different agencies regulate different industries – the Department of Health and Human Services regulates privacy in healthcare, the Department of Education regulates privacy in education, the Federal Communications Commission regulates privacy in telecommunications, and so on.

In a sectoral approach, with so many different sources of law and regulation, the FTC can play a harmonizing role. A more aggressive FTC might obviate the need for new laws. The more the FTC starts acting like a national data protection authority, the fewer gaps and fewer needs of states to protect their citizens. There seems to be practically little

---

[107] Robert Gellman, A Better Way to Approach Privacy Policy in the United States: Establish A Non-Regulatory Privacy Protection Board, 54 Hastings L.J. 1183, 1214 (2003).

[108] Communication from the Commission: Safeguarding Privacy in a Connected World: A European Data Protection Framework for the 21st Century, at 8-9, COM (2012) 9 final (Jan. 25, 2012) [hereinafter Safeguarding Privacy], available at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0009:FIN:EN:PDF; *See also* Francoise Gilbert (FNdd1), European Data Protection 2.0: New Compliance Requirements in Sight-What the Proposed Eu Data Protection Regulation Means for U.S. Companies, 28 Santa Clara Computer & High Tech. L.J. 815, 817 (2012)

chance that Congress will pass an omnibus privacy or data security regulation because of turf wars and various other infirmities with the current federal legislative process. But the sectoral approach is increasingly causing confusion and inefficiency, as well as being at variance with most of the rest of the world. The FTC's power is broad enough to develop over time a more coherent and comprehensive body of regulatory activity.

Robert Gellman has argued that the United States needs a federal privacy agency. According to Gellman, "The main objective of a privacy agency would be to promote the adoption and implementation throughout the United States of protections for personal privacy and of principles of Fair Information Practices. Other functions would include issuing advisory opinions, conducting investigations, proposing rules and legislation, commenting on governmental and private sector actions affecting privacy, assisting with private sector self-regulatory efforts, and maintaining international continuity."[109]

While Gellman's proposed privacy agency would not be regulatory, he sees great value in the harmonizing effect such an agency could have. He observed, "For present purposes, it is sufficient to assert that nearly every institution in the modern world maintains personal data and that nearly every individual is the subject of data files maintained by those institutions. Nowhere is this more true than in the United States, where the collection, maintenance, use, and disclosure of personal information is ubiquitous among private and governmental organizations….Both record keepers and record subjects share risks and responsibilities regarding the processing of personal data. A privacy agency would serve the interests of both record keepers and record subjects."[110]

However, Gellman hesitates to embrace the FTC as a data protection authority, stating "The FTC's endorsement of a diluted version of FIPs is one reason that the Commission is not a good candidate to serve a larger role in privacy policy. The Commission's privacy vision is too limited. In addition, the Commission does not have jurisdiction over many private sector, non-profit, and governmental record keepers."[111] We largely agree with Gellman that the FTC could become more robust in its data protection enforcement. Indeed, the FTC has already been moving in this direction. Moreover, specific and feasible rulemaking authority and increased jurisdiction would be key additional assets for the FTC to more effectively perform the full range of functions of a DPA.

Currently, U.S. privacy law is a fragmented mess of overlapping and inconsistent laws that make it nearly impossible for consumers to figure out how their privacy is protected. Consider how to respond to the person who asks: "How is my health data protected?" HIPAA protects "protected health information" which applies to health data held by covered entities or business associates. If the data is held by a company or person that isn't a covered entity or a business associate, it's not covered by HIPAA. It might be regulated by some state health privacy laws. Or it might not be regulated by others.

If it were held by other types of companies as part of other types of records, it could be protected in different ways. If the data were part of an education record at a school, it

[109] Robert Gellman, *A Better Way to Approach Privacy Policy in the United States: Establish A Non-Regulatory Privacy Protection Board*, 54 Hastings L.J. 1183 (2003).
[110] *Id.* at 1184.
[111] *Id.* at 1205.

would be regulated by FERPA. If it were part of a financial record held by a financial institution, it would receive a different set of protections. And so on.

Certain uses could trigger common law tort actions. There could be contract law claims in connection with some uses. If the data is involved in a data breach, the person might be entitled to notification by his or her state data breach notification law, but these laws vary considerably from state to state. For many privacy violations, there might be no protection at all. For example, if a company develops an app that uses people's health data not in connection with their physicians or hospitals, then the company does not fall under HIPAA. The company does not have a privacy policy for the app, so no protections are even promised. Indeed, this is a common practice for apps. A study by the Future of Privacy Forum, which seems representative of studies of mobile application privacy practices, found that seventy five percent of the leading mobile applications did not have a privacy policy.[112]

This is why the FTC is needed. Its broad jurisdiction would likely cover this company. The FTC could set a baseline of protections for consumer health data. Other statutes could provide additional protection and focus on specific uses, but there would at least be a baseline. Returning to the example of the company with the app collecting health data that lacks a privacy policy, the FTC has cases that indicate that the company is running afoul of Section 5. The FTC now seems to be requiring baseline security practices for all companies handling personal data. Moreover, the FTC has prohibited certain kinds of data gathering even when not inconsistent with a privacy policy. [113] The FTC could take a more aggressive approach here and hold that failure to have a privacy policy with basic privacy practices is an unfair or deceptive trade practice.

For example, the FTC has already developed a baseline standard for specific and explicit notice for certain kinds of sensitive information, such as geolocation data. In *In the Matter of Goldenshore Technologies*, the FTC alleged that a mobile flashlight application "represented, expressly or by implication, that respondents may periodically collect,

---

[112] FPF Finds Nearly Three Quarters of Most Downloaded Mobile Apps Lack a Privacy Policy, Future of Privacy Forum, http://www.futureofprivacy.org/2011/05/12/fpf-finds-nearly-three-quarters-of-most-downloaded-mobile-apps-lack-a-privacy-policy/; o Jessica Guynn, Facebook to Require Privacy Policies for All Apps in App Center, L.A. TIMES (June 22, 2012), http://articles.latimes.com/2012/jun/22/business/la-fi-facebook-ag-20120622 (stating that, in 2010, forty-five "of 101 popular apps for iPhone and Android phones … didn't provide privacy policies on their websites or inside the apps"); Geoffrey A. Fowler, Tech Giants Agree to Deal on Privacy Policies for Apps, WALL ST. J. (Feb. 23, 2012), http://online.wsj.com/news/articles/SB10001424052970203918304577239650306276074 ("[California Attorney General Kamala D.] Harris said, some 22 of the 30 most-downloaded mobile apps don't have privacy policies."); Cameron Scott, Mobile App Stores to Require, Disclose Privacy Policies, PCWORLD (Feb. 22, 2012, 5:40 PM), http://www.pcworld.com/article/250516/mobile_app_stores_to_require_disclose_privacy_policies.html ("Just 5 percent of all mobile applications offer a privacy policy, according to a study conducted by TrustE and Harris Interactive. (A developer survey conducted by the Future of Privacy Foundation found that one-third of apps offer such policies.)"); see also FTC, Mobile Privacy Disclosures 23 n.96 (2013), available at http://www.ftc.gov/sites/default/files/documents/reports/mobile-privacy-disclosures-building-trust-through-transparency-federal-trade-commission-staff-report/130201mobileprivacyreport.pdf; FTC, Mobile Apps for Kids: Disclosures Still Not Making the Grade 7 (2012) ("Of the 400 [kids] apps reviewed, only 20% (81) contained any privacy-related disclosure on the app's promotion page, on the developer website, or within the app."), available at http://www.ftc.gov/sites/default/files/documents/reports/mobile-apps-kids-disclosures-still-not-making-grade/121210mobilekidsappreport.pdf

[113] Daniel J. Solove and Woodrow Hartzog, The FTC and the New Common Law of Privacy (Aug. 19, 2013), available at http://papers.ssrn.com/sol3/papers.cfm? abstract_id=2312913.

maintain, process, and use information from users' mobile devices to provide software updates, product support, and other services to users related to the Brightest Flashlight App," yet the app "failed to disclose or failed to adequately disclose that, when users run the Brightest Flashlight App, the application transmits, or allows the transmission of, their devices' precise geolocation along with persistent device identifiers to various third parties, including third party advertising networks."[114]

According to the FTC, "These facts would be material to users in their decision to install the application."[115] Thus, failure to specifically provide notice of the collection of geolocation data was seen as deceptive. Given the high visibility of privacy concerns and the general trust and expectation of privacy by consumers, might the FTC also claim that failure to have basic privacy practices also be deceptive?

Critics of more expansive FTC enforcement might raise concern that it would be an impediment to industry and innovation. Their outcries about lack of notice and unpredictability might turn into outright shrieks if the FTC started to adopt standards that were more in the gray zone, where consensus might be less widespread. Companies might find it harder to know what they must do to be compliant.

The state of data protection today, however, is significantly different than it was a decade ago, let alone two decades ago. Industry standards have evolved and matured, and there is a robust group of privacy professionals, academics, advocates, and others who can provide feedback. Early on, a more restrained approach better fit with the fact that so much was new and there were not many people to guide industry. Now guidance has been established by a privacy profession and a privacy bar. One reason why the FTC can take a bolder approach is that now companies have access to expertise and resources to better help them comply.

2. The FTC's Diverse Toolkit

One of the reasons the FTC is so critical in the modern privacy regulatory scheme is that it is has a considerably broad and diverse toolkit from which to fashion remedies which allows the commission to redress non-traditional forms of harm, balance data protection against countervailing interests in ways that other areas of law are currently unable to do, and create proactive solutions like those that rely upon design obligations to decrease risks of privacy and security harms ex ante.

(a)Redress for Non-Traditional Forms of Harm

Contract law and tort law have thus far not been frequently successfully applied to many of the issues involving the collection, storage, use, and disclosure of personal data.[116] When contract and tort have been applied to these issues, courts have struggled significantly in the application.[117] More broadly, the law has struggled to recognize

---

[114] In the Matter of Goldenshores Technlologies, http://www.ftc.gov/sites/default/files/documents/cases/131205goldenshorescmpt.pdf.
[115] *Id.*
[116] *See, e.g.*, Dwyer v. American Express Co., 652 N.E.2d 1351 (Ill. App. 1995); In re iPhone Application Litigation, 844 F.Supp.2d 1040 (N.D. Cal. June 12, 2012); Dyer v. Northwest Airlines Corp., 334 F. Supp. 2d 1196 (D.N.D. 2004); In re Jet Blue Airways Corp. Privacy Litigation, 379 F. Supp. 2d 299 (E.D.N.Y. 2005).
[117] *Id.*

privacy violations and data security breaches as harms.[118] The United States Court of Appeals, Third Circuit observed that "In this increasingly digitized world, a number of courts have had occasion to decide whether the "risk of future harm" posed by data security breaches confers standing on persons whose information may have been accessed. Most courts have held that such plaintiffs lack standing because the harm is too speculative."[119]

In rejecting the appellant's contention that an increased risk of identity theft is itself a harm, the court stated that the appellants "have alleged no misuse, and therefore, no injury. Indeed, no identifiable taking occurred; all that is known is that a firewall was penetrated. Appellants' string of hypothetical injuries do not meet the requirement of an 'actual or imminent' injury."[120] While this logic has begun to be chipped away by some courts,[121] few plaintiffs are able to succeed in tort and contract-based claims for harm resulting from a data breach without concrete evidence of financial harm like credit card fraud or identity theft.[122]

In most other domains of law, harm can be hard to establish because data protection violations often do not lead to immediate physical or financial injury. For example, in the recent opinion dismissing a claim against Nationwide Mutual Insurance for poor data security practices, a U.S. District court refused to recognize an increased risk of harm/cost to mitigate increased risk, a loss of privacy and deprivation of the value of PII as actionable harms to provide the plaintiffs with standing to bring a negligence, invasion of privacy and bailment claims.[123] Regarding increased risk of future harm, the court held that "In this case, an increased risk of identity theft, identity fraud, medical fraud or phishing is not itself an injury-in-fact because Named Plaintiffs did not allege—
or offer facts to make plausible—an allegation that such harm is 'certainly impending.'"[124] Regarding the cost to mitigate the risk of harm, the court held that "Such injury does not suffice to confer standing because 'respondents cannot manufacture standing merely by inflicting harm on themselves based on their fears of hypothetical future harm that is not certainly impending.'"[125]

The court in *Galaria* similarly rejected plaintiff's loss of privacy theory of harm, stating "Named Plaintiffs failed to allege that the loss of privacy has itself resulted in any adverse consequences apart from the speculative injury of increased risk of identity theft,

---

[118] Reilly v. Ceridian Corp., 664 F.3d 38 (3d Cir. 2011) ("Appellants' contentions rely on speculation that the hacker: (1) read, copied, and understood their personal information; (2) intends to commit future criminal acts by misusing the information; and (3) is able to use such information to the detriment of Appellants by making unauthorized transactions in Appellants' names. Unless and until these conjectures come true, Appellants have not suffered any injury; there has been no misuse of the information, and thus, no harm.").
[119] Reilly v. Ceridian Corp., 664 F.3d 38, 43 (3d Cir. 2011).
[120] Reilly v. Ceridian Corp., 664 F.3d 38, 44 (3d Cir. 2011).
[121] *See e.g.*, Resnick v. AvMed, Inc., 693 F.3d 1317 (11th Cir. 2012); Cousineau v. Microsoft Corp., No. C11-1438-JCC (W.D. Wash. June 22, 2012), *available at* http://newsandinsight.thomsonreuters.com/uploadedFiles/Reuters_Content/2012/06_June/gibson_microsoft.pdf; Anderson v. Hannaford Bros., 659 F.3d 151, 166–67 (1st Cir. 2011).
[122] *See, e.g.*, Katz v. Pershing, LLC, 672 F.3d 64 (1st Cir. 2012); Amburgy v. Express Scripts, Inc. 671 F. Supp. 2d 1046 (E.D. Mo. 2009); LaCourt v. Specific Media, Inc., No. SACV 10-1256-GW, 2011 WL 1661532 (C.D. Cal. Apr. 28, 2011).
[123] Opinion and Order, Galaria v. Nationwide Mutual Insurance Co., Case No. 2:13—cv-118.
[124] *Id.* at 11-14 (referencing Clapper v. Amnesty Intern. USA, 133 S.Ct. 1138, 1142-43 (2013)).
[125] *Id.* at 18 (citing Clapper v. Amnesty Intern. USA, 133 S.Ct. 1138, 1143, 1151 (2013)).

identity fraud, medical fraud, or phishing."[126] The court was simply unwilling recognize harm for standing purposes regardless of whether data "is ever actually misused or the plaintiff ever suffers adverse consequences from the exposure."[127] Finally, the court rejected the plaintiff's argument that "they suffered an injury-in-fact in the form of deprivation of the value of their PII."[128] The court was skeptical of the argument that PII has any inherent monetary value and stated that "Regardless of whether Named Plaintiffs argue the value of their PII has merely diminished or whether they allege complete deprivation of value, they have failed to allege any facts explaining how their PII became less valuable to them (or lost all value) by the data breach."[129] The court appeared to want evidence of the market's response to compromised data, stating "neither Named Plaintiff alleges he tried to sell his PII after the data breach but was unable to do so because of the breach or was forced to sell it for less than its full worth. Nor does either Named Plaintiffallege that any third party sold his PII and that Named Plaintiff was deprived of his rightful profit."[130]

In contrast, the FTC can regulate with a much different and more flexible understanding of harm. In its statement on unfairness, the FTC states specifically that "An injury may be sufficiently substantial, however, if it does a small harm to a large number of people, or if it raises a significant risk of concrete harm."[131]

Harm is a specifically acute problem with respect to data breaches. What is the harm when data is leaked? This question has confounded courts, which often don't recognize a harm. If people's credit cards are just cancelled and replaced, and they do not pay anything, are they harmed? If people's data are leaked, but they do not suffer from identity theft, are they harmed? Although courts struggle to recognize harm, there clearly seems to be a substantial negative impact on people's lives. The harm of credit card fraud is that it can take a long time to replace all the credit card information in various accounts. People have card data on file with countless businesses and organizations for automatic charges and other transactions. Replacing all this data can be a major chore. People's time has a price. That price will vary, but it rarely is zero.

A data breach also causes a harm because people are at greater risk for fraud and will feel anxiety and concern. People might reasonably spend money and time to protect themselves. One problem is that recognizing harm can be a Hobson's choice for courts. Recognize harm, even a tiny one, and there's a floodgate of class action suits and damage awards that could total billions because of the enormous numbers of people whose data is affected in a breach. A small harm multiplied by tens of millions of people can really add up to catastrophic damages for a company. Failing to recognize harm is bad, too, because there really is harm, and it needs to be appropriately deterred and redressed.

Harm from a data breach is a central issue in *FTC v. Wyndham*. Wyndham claimed in its motion to dismiss that "Because federal statutes and card-brand rules eliminate the possibility that consumers can suffer financial injury from the theft of payment-card data,

---

[126] *Id.* at 21.
[127] *Id.*
[128] *Id.*at 22.
[129] *Id.* at 24-25.
[130] *Id.*at 25.
[131] FTC Policy Statement on Unfairness, Appended to International Harvester Co., 104 F.T.C. 949, 1070 at fn12 (1984). See 15 U.S.C. § 45(n).

practices regarding the security of that data cannot trigger the necessary precondition of FTC jurisdiction—namely, that there be 'substantial injury to consumers which is not reasonably avoidable by consumers themselves.'"[132] The FTC responded that there only need be a likelihood of injury though actual financial losses had been pled and that another forms of unavoidable injury that occurred due to the breach included "unreimbursed fraud charges, the loss of access to funds as a result of frozen or depleted bank accounts, even if temporary, temporary loss of access to credit, and the cost of reasonable mitigation [including] time, trouble and aggravation dealing with unwinding this fraud, and with re-establishing recurring payments after the credit cards have to be changed for hundreds of thousands of consumers."[133] In *FTC v. Neovi*, the Ninth Circuit supported the district court's finding that "It is likely that some consumers never noticed the unauthorized withdrawals. Even if the consumer did notice, obtaining reimbursement required a substantial investment of time, trouble, aggravation, and money. Further, Defendants' uncooperativeness only increased this outlay. Neither could consumers mitigate the period of time during which they lost access to and use of the funds taken using Defendants' fraudulent checks. Regardless of whether a bank eventually restored consumers' money, the consumer suffered unavoidable injuries that could not be fully mitigated."[134]

In a remarkable footnote in Judge Salas's opinion in *Wyndham* recognizing the dispute over whether non-monetary injuries are cognizable under Section 5, the court seemed amendable to recognizing non-monetary harm: "Although the court is not convinced that non-monetary harm is, as a matter of law, unsustainable under Section 5 of the FTC Act, the Court need not reach this issue given the substantial analysis of the substantial harm element above."[135]

It is a mistake to assume that the only cognizable injuries from data breaches are financial. One important kind of harm enabled by data breaches that has been overlooked by many is the use of consumers own personal information to trick them. For example, pieces of information like social security numbers, telephone numbers, and even credit card numbers are often used to verify an Internet user's identity. Malicious actors in possession of such personal information have a much easier time engaging in "phishing" attacks against the subject of the data as well as those within the subject's social network by spoofing legitimate requests for even more personal and sensitive information. Consumers are less likely to question the authenticity of a source in possession of such identifying information because it would appear as though a legitimate source was simply using the information provided by the customer or that the communication was coming

---

[132] Motion to Dismiss by Wyndham Hotels & Resorts LLS, FTC v. Wyndham Worldwide Corp., No. 2:12-cv-01365-SPL at 8 (D. Ariz. filed Aug. 27, 2012).

[133] Transcript of Oral Argument, FTC v Wyndham, pg. 126, *available at* http://www.pogowasright.org/wp-content/uploads/FTC_V._WYNDHAM_OralArgument-.pdf; It is important to note that some courts have explicitly rejected similar theories of harm for tort and contract based. *See, e.g.,* Reilly v. Ceridian Corp., 664 F.3d 38, 46 (3d Cir. 2011) ("Although Appellants have incurred expenses to monitor their accounts and "to protect their personal and financial information from imminent misuse and/or identity theft," App. 00021, they have not done so as a result of any actual injury (e.g. because their private information was misused or their identities stolen). Rather, they prophylactically spent money to ease fears of future third-party criminality. Such misuse is only speculative—not imminent. The claim that they incurred expenses in anticipation of future harm, therefore, is not sufficient to confer standing.").

[134] F.T.C. v. Neovi, Inc., 604 F.3d 1150, 1158 (9th Cir. 2010) amended, 09-55093, 2010 WL 2365956 (9th Cir. June 15, 2010).

[135] FTC v. Wyndham Worldwide Corp., No. 13-1887 Slip Op. (April 7, 2014 D.N.J.) at 28, footnote 15.

from or endorsed by a friend. This practice can be difficult to discover and track, yet could lead to the mistaken disclosure of personal information due to deception and frustration of consumer choice, the tenets of the FTC's Section 5 prohibitions on deceptive and unfair trade practices.

The FTC is also unique in that it has the tools and the motivation to protect vulnerable populations and has aimed much of its enforcement against those who would seek to unfairly manipulate parties by exploiting inherent biases and vulnerabilities. Much of the FTC's enforcement against false advertising is against those would exploit the elderly. In the realm of privacy, the Children's Online Privacy Protection Act (COPPA) was created to protect minors because they are seen as less capable of making informed decisions regarding disclosing personal information online.

But this focus on vulnerability places the FTC in a unique position to respond to those who would exploit the human tendency to make irrational decisions. While such actions might not be recognized as a traditional privacy harm, a growing body of research is showing how such practices, if unregulated, could ultimately harm consumers, perhaps even in ways they do not even realize.[136]

Another key benefit is that the FTC need not wait for evidence of actual harm before it brings a complaint, unlike other regulatory regimes. Recall that the injury required for unfairness may be sufficiently substantial if "raises a significant risk of concrete harm."[137] As defined by Section 5, "unfair and deceptive trade practices" includes "such acts or practices involving foreign commerce that…cause or are *likely to cause* reasonably foreseeable injury within the United States."[138] Many privacy and data security harms are not immediately experienced. Data is leaked or exposed and might be obtained for fraud a while later. With certain kinds of personal data, there is no expiration date – the data can be used for fraud now or many years in the future. Privacy and data security are predominantly about risk. Risk is a concept that the law often struggles with, because the law is still shackled with its more primitive foundations where it focused on more tangible and immediate things. This makes the FTC one of the few regulatory options for probabilistic theories of privacy harm.

(b). Balancing that Accounts for Larger Societal Interests

Another great challenge with privacy and data security cases is that the harms of violations are often quite dispersed and have a more of a societal impact than an impact on any one individual. The FTC has better tools than those that exist in many other areas of law to address this kind of impact.

Although an individual can certainly suffer significant harm from a data protection violation, in many cases, the harm might be small or difficult to measure. Harm from data protection violations can also build up from the collective actions of a multitude of actors. In a previous work, one of us likened many data protection violations to a bee

[136] *See* M. Ryan Calo, Digital Market Manipulation, George Washington Law Review (forthcoming); Daniel J. Solove, *Privacy Self-Management and the Consent Dilemma*, 126 Harv. L. Rev. 1880 (2013).
[137] FTC Policy Statement on Unfairness, supra note ^, at fn 12.
[138] 15 U.S.C. § 45(a)(4)(a) (emphasis added).

sting. "One bee sting can be shrugged off, but a hundred or a thousand can be lethal."[139] With each sting, the law typically turns its back and finds the harm not worth addressing. But if the stings are not redressed, they collectively can take a greater toll. Many areas of law are incapable of looking at the larger picture; they myopically focus on the trees and forget that each tree is part of the forest.

FTC jurisprudence on injury has a broader focus than that of many other legal domains. According to the FTC, even incremental harms that affect a large group of consumers can be substantial. Indeed, this seems to be one of the contemplated categories of "substantial injury" from an unfair practice.[140] In determining whether an injury is outweighed by any countervailing benefits to consumers or competition, the FTC considers not only the consumer's cost to remedy the alleged injury, but also the cost to society in general.[141] According to the FTC, "These societal costs exist in the form of 'increased paperwork, increased regulatory burdens on the flow of information, reduced incentives to innovation and capital formation, and similar matters.'"[142]

The FTC is able to consider a more complete range of concerns than much of contract and tort law, and it is thus able to come to a balance that is more subtle and comprehensive of everything at stake. In evaluating unfairness, the FTC considers whether a trade practice violates established public policy "as it has been established by statute, common law, industry practice, or otherwise."[143] This factor is usually used to help determine whether a consumer injury is substantial.

The FTC thus has a broader and more nimble conception of harm that tort, contract, and many statutes. In many privacy and data security cases, there is a strained discussion of harm that tries to squeeze data protection harms into concepts poorly designed to accommodate the nature of these harms. The FTC can avoid this morass because its conception of harm is well-suited to data protection cases.

(c). Ameliorating Privacy Harms from Institutional Bargaining

The FTC can also mitigate the negative effects that intuitional bargaining has on consumers privacy. Increasingly, consumers relationships with companies are negotiated through institutions, yet consumers are at the mercy of those organizations negotiating their fate. For example, K-12 schools as well as colleges/universities negotiate contacts with cloud service providers and other data services, and these contracts often fall short of protecting student privacy.[144]

---

[139] Daniel J. Solove, *Privacy Self-Management and the Consent Dilemma*, 126 Harv. L. Rev. 1880, 1891 (2013).

[140] F.T.C. v. Neovi, Inc., 604 F.3d 1150, 1157 (9th Cir. 2010) amended, 09-55093, 2010 WL 2365956 (9th Cir. June 15, 2010) ("An act or practice can cause "substantial injury" by doing a "small harm to a large number of people, or if it raises a significant risk of concrete harm.") (citing Am. Fin. Servs. Ass'n v. FTC, 767 F.2d 957, 972 (D.C.Cir.1985) (quotation marks and citations omitted) cert. denied, *1158 475 U.S. 1011, 106 S.Ct. 1185, 89 L.Ed.2d 301 (1986)).

[141] FTC Policy Statement on Unfairness, supra note ^.

[142] FTC Policy Statement on Unfairness, Appended to International Harvester Co., 104 F.T.C. 949, 1070 (1984).

[143] *Id.*

[144] Daniel Solove, Why Schools Are Flunking Privacy and How They Can Improve, LinkedIn (Dec. 17, 2013), http://www.linkedin.com/today/post/article/20131217054543-2259773-why-schools-are-flunking-privacy-and-how-they-can-improve?trk=mp-reader-card.

A study conducted by Fordham School of Law's Center on Law and Information Policy (CLIP) revealed that contracts between K-12 school districts and cloud service providers lacked essential terms for the protection of student data.[145]

Many of the agreements analyzed failed to give the school districts the right to audit and inspect the vendor's practices with respect to the transferred data.[146] The agreements also failed to prohibit or limit re-disclosure of student data or other confidential information.[147] No agreement "specifically prohibited the sale and marketing of children's information."[148].

Consumers are caught in the cross fire, because their interests are often ignored in these contracts unless the schools fight for them. In the context of schools, the Department of Education (DoE) under FERPA has very little ability to do much about it, and unlike HHS, the DoE has no direct authority to regulate companies receiving education records.[149]

Currently, the FTC is likely unable to regulate non-profit schools as they are likely not engaged in "commercial" activity.[150] However, in similar situations involving for-profit companies, the FTC has held that a company's failure to adequately choose, contract with, and oversee a data service provider constituted an unfair and deceptive trade practice. The case, *In the Matter of GMR Transcription Services, Inc.*, involved the inadvertent exposure of people's medical data maintained by GMR, a company that provides medical transcription services.[151] According to the FTC complaint, GMR failed to "adequately verify that their service provider, Fedtrans, implemented reasonable and appropriate security measures to protect personal information in audio and transcript files on Fedtrans' network and computers used by Fedtrans' typists."[152] Moreover, the FTC faulted GMR for failures in contracting with its data service provider. The FTC complaint alleged that GMR failed to "require Fedtrans by contract to adopt and implement appropriate security measures to protect personal information in medical audio and transcript files, such as by requiring that files be securely stored and securely transmitted

[145] For example, The report begins by noting that 95% of school districts use cloud services. They are sharing sensitive student data with these third party cloud service providers. Yet "approximately 20% of the responding districts had no policies addressing teacher use of information resources." *Id.*
[146] *Id.* at 25.
[147] *Id.* at 28.
[148] *Id.*at 28.
[149] *See* Bryan Thurmond, Dismantling A Dual-Headed System of Governance: How A Regulatory Overlap Undercuts the Security of Student Health Information in Public Schools, 64 ADMIN. L. REV. 701, 707 (2012) ("[A]s spending legislation, [the Department of Education] enforces FERPA's provisions through the disbursement or rescission of federal education funds."); Benjamin F. Sidbury, Gonzaga University v. Doe and Its Implications: No Right to Enforce Student Privacy Rights Under Ferpa, 29 J.C. & U.L. 655, 657 (2003) (footnote omitted) (citations omitted) ("[T]he language of [20 U.S.C. § 1232g(b)(1)] suggests that FERPA does not impose a per se prohibition on the disclosure of educational records to third parties but merely imposes a funding precondition such that an institution will not receive federal funding if the institution has a 'policy or practice of permitting the release of education records.' An institution, therefore, stands to lose all or a portion of its federal funding if it has a policy or practice of disclosing its students' educational records to unauthorized third parties." (quoting 20 U.S.C. § 1232g(b)(1))).
[150] California Dental Ass'n v. FTC, 526 US 756, 766-67 (1999) and Community Blood Bank v. FTC, 405 F.2d 1011, 1012 (8th Cir. 1969).
[151] In the Matter of GMR Transcription Services, Inc.,, Complaint, http://www.ftc.gov/system/files/documents/cases/140203gmrcmpt.pdf.
[152] *Id.*

to typists (e.g., through encryption) and authenticating typists (e.g., through unique user credentials) before granting them access to such files; take adequate measures to monitor and assess whether Fedtrans employed measures to appropriately protect personal information under the circumstances."[153]

The FTC additionally found GMR to be deficient in doing due diligence before hiring its data service provider. Looking broadly at the complaint, there are three key things that the FTC is now requiring companies to do when it comes to contracting with data service providers: (1) exercise due diligence before hiring data service providers; (2) have appropriate protections of data in their contracts with data service providers; and (3) take steps to verify that the data service providers are adequately protecting data.[154]

Because the FTC's Section 5 power is generally limited to commercial entities, the FTC lacks the ability to enforce similar responsibilities on school districts. We believe that the FTC should have authority over non-commercial entities that engage in practices that result in consumer harm.

However, the lack of such authority does not need to preclude the FTC from becoming involved, as the FTC can bring enforcement actions against the vendors that enter into such deficient contracts with schools. In *In re Vision I Properties,* the FTC brought an action against Vision I Properties, a company that provided software that created customized shopping cart pages for other companies. Vision I rented people's personal data collected through its software to direct marketers. This was in violation of some of the privacy policies of the companies using Vision I's software. Even though Vision I was not violating its own privacy policy, the FTC concluded that it thwarted consumer expectations formed based upon the privacy policies of the other companies. The import of this case is that the FTC did not see this scenario as involving merely an arrangement between Vision I and other companies. Consumers were caught in the middle, and the FTC ensured that their interests would not be lost in the relationship. Thus, a relationship between a school district and a company providing data services that harms consumers might justify FTC enforcement action. Consumers need not have a direct relationship to companies that cause them harm. Combining *Vision I* with *GMR* suggests that consumers can be harmed when the appropriate contractual protections are not included in agreements involving the sharing of personal data.

The FTC has already developed a theory of data security that requires companies holding personal information to ensure that third party recipients will safeguard any data the company shares.[155] Specifically, the FTC has filed complaints of unfairness against

---

[153] *Id.*
[154] *Id.*
[155] *See* Daniel J. Solove & Woodrow Hartzog, *The FTC and Privacy and Security Duties for the Cloud*, 13 BNA Privacy & Security Law Report 577 (2014). For examples of FTC critiques of inadequate third-party access control, see, e.g., Wyndham Complaint, supra note ^, at 12; Rental Research Servs. Complaint, supra note ^, at 7; ValueClick Complaint, supra note ^, at 5; Upromise Complaint, supra note ^, at 4--5; ACRAnet Complaint, supra note supra note ^, at 2; Premier Capital Lending Complaint, supra note ^, at 3--4; Nations Title Agency Complaint, supra note ^, at 2. This includes failure to verify and authenticate the identities of third-party recipients as well as failure to monitor or otherwise identify unauthorized recipient activity. See Complaint for Civil Penalities, Permanent Injunction, and Other Equitable Relief at 4, United States v. ChoicePoint Inc., No. 06-CV-0198 (N.D. Ga. Jan. 30, 2006), available at http://www.ftc.gov/os/caselist/choicepoint/0523069complaint.pdf (on file with the authors) (discussing defective verification policies). It includes general charges of failing to protect information in the hands of

companies it alleged failed to verify and authenticate identity of third-party recipients,[156] failed to monitor data recipient's activity,[157] and failed to require by contract third party protection of information.[158] Elsewhere, we have noted that there are two emerging strands of FTC jurisprudence that can address the consumer vulnerabilities inherent in institutional bargaining.[159] We noted, "The first pertains to data stewardship for the organizations that share personal data with cloud service providers. And the second pertains to third-party beneficiaries, where the FTC has recognized that consumers need not be a primary party to a contract in order to receive protection under the FTC Act."[160] We argue that these two strands are essentially flip sides of the same coin. Under this approach, data collectors must act as data stewards and protect consumers when the organization shares information with third party data handler. Likewise, the third party data recipient and processor also owes a duty to consumers, who are essentially third-party beneficiaries of the data collector's efforts to ensure privacy and data security in their institutional bargaining.[161]

The FTC could adopt a similar approach with respect to privacy-based requirements like requirements for confidentiality and data minimization and prohibitions on reidentification, data mining, and certain kinds of advertising and marketing to those identified in the data.

III. THE LIMITS OF FTC POWER AND ESSENTIAL IMPROVEMENTS

What are the limits of FTC power? What limits should there be on FTC power? Thus far, we have argued that the FTC enjoys very broad powers for data protection enforcement and that the FTC should use these powers more robustly. But, of course, there are legal limits to how far the FTC can go. And there are certainly reasons for some degree of caution. In this section, we discuss what the FTC is unable to do and what the FTC should avoid doing.

We argue that although the FTC should certainly hit the accelerator and move beyond being very conservative in its enforcement, the FTC should be careful not to become too much of what Cass Sunstein and others have referred to as a "norm entrepreneur."[162] We also discuss certain shortcomings in existing FTC enforcement practices that should be improved. We argue that if the FTC is to embrace a greater role in data protection, it must be more transparent in defining the contours of Section 5. The FTC must also be more proportionate in its enforcement of Section 5 to reflect the full range of actions that

---

third party recipients as well as very specific charges by the FTC such as "[f]ailing to oversee service providers and to require them by contract to implement safeguards to protect respondent's customer information." Nations Title Agency Complaint, supra note ^, at 4.

[156] See, e.g., ChoicePoint Complaint, supra note ^, at 5 (admonishing company for accepting contradictory verification documentation).

[157] See ChoicePoint Complaint, supra note ^, at 9--10.

[158] This is also a violation of the GLBA Safeguards Rule. See, e.g., Sunbelt Lending Servs., Inc., 139 F.T.C. 1, 2--3 (2005) (complaint) (analyzing violations of Safeguards Rule); Nations Title Agency Complaint, supra note ^, at 3--4 (same).

[159] Daniel J. Solove & Woodrow Hartzog, *The FTC and Privacy and Security Duties for the Cloud*, 13 BNA Privacy & Security Law Report 577 (2014).

[160] *Id.*

[161] *Id.*

[162] Cass R. Sunstein, Social Norms and Social Roles, 96 Colum. L. Rev. 903, 909 (1996).

constitute unfair and deceptive trade practices. Such changes are necessary to better encourage companies to act fairly and honestly. They are also necessary to better enable all companies, even those with limited resources, to proactively protect consumer data.

A. The Limits of Section 5 Authority

The FTC's Section 5 authority is not boundless. As previously indicated, the FTC lacks jurisdiction over banks, savings and loan institutions, Federal credit unions, common carriers, air carriers, meat packers, and non-profit entities.[163] Additionally, the previously mentioned requirements of materiality, balancing, and harm facially limit the scope of valid complaints alleging unfair and deceptive trade practices.

Under the Administrative Procedure Act, the FTC is also prohibited from acting arbitrarily, capriciously, or abusing its discretion.[164] Although actions must be extreme to be labeled arbitrary, capricious, or an abuse of authority, this limit prohibits a blind disregard the FTC's delegated power.[165]Jeff Sovern has noted that:

> [T]he FTC Act itself limits the FTC to some degree by providing that the FTC may bring only proceedings which "would be to the interest of the public. . . ." While courts usually defer to the FTC on which actions are in the public interest, and thus the public interest requirement is not a terribly stringent limitation, courts claim they will overturn an FTC action if they find an abuse of discretion.[166]

The First Circuit recently stated that "The APA requires a reviewing court to set aside an agency decision when the administrative record shows that the decision is 'arbitrary, capricious, an abuse of discretion, or otherwise not in accordance with law.'…An agency decision fails to pass this test if the administrative record reveals that 'the agency relied on improper factors, failed to consider pertinent aspects of the problem, offered a rationale contradicting the evidence before it, or reached a conclusion so implausible that it cannot be attributed to a difference of opinion or the application of agency expertise.'"[167]

---

[163] 15 U.S.C. §45(a)(1)-(2). Non-profit entities are ostensibly not engaged in "commerce."

[164] 5 U.S.C. §§ 701-706.

[165] Am. Horse Prot. Ass'n, Inc. v. Lyng, 812 F.2d 1, 4 (D.C. Cir. 1987) ("Review under the 'arbitrary and capricious' tag line … encompasses a range of levels of deference to the agency, … and…surely reinforces our frequent statements that an agency's refusal to institute rulemaking proceedings is at the high end of the range. Such a refusal is to be overturned 'only in the rarest and most compelling of circumstances,' which have primarily involved 'plain errors of law, suggesting that the agency has been blind to the source of its delegated power.'") (citations omitted); Comment, Abuse of Discretion: Administrative Expertise vs.judicial Surveillance, 115 U. Pa. L. Rev. 40, 41 (1966) ("The question of what constitutes abuse of discretion, however, is not an easy one.").

[166] Jeff Sovern, Private Actions Under the Deceptive Trade Practices Acts: Reconsidering the Ftc Act As Rule Model, 52 Ohio St. L.J. 437, 441-42 (1991).

[167] Atieh v. Riordan, 727 F.3d 73, 75-76 (1st Cir. 2013) (quoting Assoc. Fisheries of Me. v. Daley, 127 F.3d 104, 109 (1st Cir. 1997)); *see also* Henry v. I.N.S., 74 F.3d 1, 4 (1st Cir. 1996) (citations omitted) ("We have pointed out that courts can abuse discretion in any of three aspects, namely, by neglecting to consider a significant factor that appropriately bears on the discretionary decision, by attaching weight to a factor that does not appropriately bear on the decision, or by assaying all the proper factors and no improper ones, but nonetheless making a clear judgmental error in weighing them."); Star Fruits S.N.C. v. United States, 393 F.3d 1277, 1281 (Fed. Cir. 2005) ("An abuse of discretion [under the APA] occurs where the decision is based on an erroneous interpretation of the law, on factual findings that are not supported by substantial evidence, or represents an unreasonable judgment in weighing relevant factors." (citing Arnold P'ship v.

As previously noted, the FTC must also provide fair notice to those it regulates. Gerard M. Stegmaier and Wendell Bartnick note that "The fair notice doctrine requires that entities be able to reasonably understand whether their behavior complies with the law. If an entity acting in good faith cannot identify with "ascertainable certainty" the standards to which an agency expects it to conform, the agency has not provided fair notice."[168]

While a reasonableness requirement tethered to industry standards is a common and acceptable practice, presumably the FTC would run afoul of fair notice problems if it disassociated its reasonableness mandate from standards that are commonly understood by those in the context in which they are regulated. If the FTC were to reject industry standards and obligate companies to act in a way that significantly deviated from reasonable, responsible companies, it would presumably be required to provide more specific guidance—perhaps even to the point of being obligated to create specific rules.

Critics allege that they are wholly without guidance for what constitutes fair data security practices. But the FTC's requirements have not been forged arbitrarily or out of whole cloth. Because the FTC, like numerous other federal and state statutes, has tethered its data security obligations to industry standards, guidance is plentiful.

B. The Appropriate Level of Restraint

As we have argued earlier, the FTC has been rather conservative in its enforcement, eschewing the role of being a norm entrepreneur. There are likely many reasons for this restraint, including a deference to some self-regulatory efforts, limited resources and political considerations. Thus, the FTC's conservative approach has brought considerable benefits, and has been quite wise. But the fact that this approach has worked in the past does not mean that it is best suited for the future.

We contend that the FTC should not continue on with the same level of restraint that it has done thus far. In the early days of FTC data protection enforcement, so many privacy norms had yet to develop. Most companies lacked privacy officers. There was barely a privacy bar. In contrast, today there is an established support system of privacy professionals dedicated to helping companies understand their obligations under certain privacy regimes like the FTC. Andrew Clearwater and Trevor Hughes wrote, "From essentially no active professionals in the 1970s and 1980s, the privacy profession has grown to at least 13,000 people working on managing information privacy within their organizations. As the information economy continues to grow-pushed by the breath-

---

Dudas, 362 F.3d 1338, 1340 (Fed. Cir. 2004)); Diaz-Resendez v. I.N.S., 960 F.2d 493, 495 (5th Cir. 1992) (citations omitted) (noting that an agency's "decision may be reversed as an abuse of discretion when it is made without rational explanation, or inexplicably departs from established policies"); Managed Pharmacy Care v. Sebelius, 716 F.3d 1235, 1244 (9th Cir. 2013) cert. denied, 134 S. Ct. 900 (U.S. 2014) and cert. denied, 134 S. Ct. 986 (U.S. 2014) (noting that the "arbitrary, capricious, an abuse of discretion, or otherwise not in accordance with law" standard of 5 U.S.C. § 706(2)(A) "is met only where the party challenging the agency's decision meets a heavy burden of showing that 'the agency has relied on factors which Congress has not intended it to consider, entirely failed to consider an important aspect of the problem, offered an explanation for its decision that runs counter to the evidence before the agency, or is so implausible that it could not be ascribed to a difference in view or the product of agency expertise.'" (quoting Motor Vehicle Mfrs. Ass'n v. State Farm Mut. Auto. Ins. Co., 463 U.S. 29, 43 (1983)).

[168] Gerard M. Stegmaier, Wendell Bartnick, Another Round in the Chamber: Ftc Data Security Requirements and the Fair Notice Doctrine, 17 J. Internet L. 1, 19 (2013).

taking speed of technological development, cloud computing, big data, and emerging uses for exponentially increasing stores of data-it is reasonable to expect that the privacy profession will grow."[169] These counselors have a nuanced understanding of the significance of the FTC complaints and are able to rely on the FTCs guidance as well as industry standards to competently advise their clients. In short, the system is primed and ready for the FTC to take on a bigger role.

The threats to privacy posed by the digital age are no longer novel, yet privacy law has yet to adequately respond to many of them. With an established regulatory compliance support system in place and a grant of power well-suited to tackle the slipperiest aspects of privacy law, the time has come for the FTC to fulfill its potential.

The viability of FTC's role and the extent of its influence depends upon privacy professionals. The FTC has limited resources and can only pursue a few cases each year. One reason it is able to achieve such power without having to bring thousands of cases each year is that privacy professionals review the FTC's activities and take steps to comply. In-house privacy counsel have an incentive to stay ahead of the FTC and avoid regulatory trouble for their organizations. They help bring the FTC's activities to the attention of the C-Suite, who otherwise might not be aware of what the FTC is doing or why it matters. Outside counsel also advise on the FTC's activities. Whenever the FTC resolves a new case, the privacy bar goes aflutter, and blog posts are written on blogs of large law firms, as well as updates in various other media forums. In other words, whenever the FTC speaks, the privacy bar amplifies it and spreads the word. They help encourage companies to comply.

However, the FTC should be careful to avoid embracing norms that lack a fair degree of consensus. Sunstein has written that "Existing social conditions are often more fragile than might be supposed, because they depend on social norms to which -- and this is the key point -- people may not have much allegiance. What I will call norm entrepreneurs -- people interested in changing social norms -- can exploit this fact."[170] So far, the FTC has served as more of a standard codifier than a standard maker. Instead of blazing a trail by creating new norms and standards, the FTC has waited until norms and standards have developed and then begun enforcement.

Once the FTC has enforced based on a particular standard, that standard achieves a new level of legitimacy and formality. For all intents and purposes, the standard becomes law. Because the law of privacy and data security is so fragmented, so magma-like in its nature, the FTC has had an unusually influential role in shaping the law of privacy and data security by embracing certain standards and norms that have achieved a decent level of consensus. The FTC should certainly push toward the logical implications of certain norms, but it must be careful not to be too radical. There must be a foundation.

The FTC is also subject to political pressure. In describing some practical restraints on the FTC, Sovern has noted that Congress has the power to limit FTC power if the FTC

[169] Andrew Clearwater, J. Trevor Hughes, In the Beginning . . . an Early History of the Privacy Profession, 74 Ohio St. L.J. 897, 898 (2013). The International Association of Privacy Professionals, one of the largest associations of its kind, recently enrolled its 15,000th member. *See* Sam Pelfie, IAPP Hits 15k Members, IAPP (Feb. 13, 2014), https://www.privacyassociation.org/publications/iapp_hits_15k_members.
[170] Cass R. Sunstein, Social Norms and Social Roles, 96 Colum. L. Rev. 903, 909 (1996).

oversteps, and that the FTC has budget and staff limitations and thus is :unlikely to expend its scarce resources on trivial deceptions."[171]

So there is good reason not to completely abandon the panoply of other remedies for privacy harms. Although the FTC can certainly play a larger role in the privacy regulatory ecosystem, it is not capable of shouldering the entire burden of protecting personal information.

Moreover, there are certain types of harm that the FTC is not as well-poised to redress. For example, compensatory remedies are also better suited for torts or other statutes because the FTC's role is largely to discourage bad behavior. The FTC also operates under significant resource constraints, and has generally brought only about ten to twenty five privacy and data security cases per year.[172]

C. Areas for Improvement

If the FTC is going to develop its jurisprudence in an incremental and bottom-up way similar to the common law, it must to a better job articulating the metes and bounds of Section 5. While the FTC provides a fair amount of information in many of its complaints, it could do more. Often, discussions of harm and balancing are either marginalized or completely absent from complaints alleging unfairness. If the FTC's incremental approach is to be fully embraced, it should better recognize the fact that many companies and counselors rely on its complaints to shape guidance and behavior.

To properly proceed in an incremental and bottom up fashion, the FTC should be more transparent about the investigations that result in a finding of fair and truthful trade practices. While companies receive notice of complaints actually filed by the FTC, they usually do not get the benefit of knowing when an FTC investigation did not result in the filing of a complaint. The FTC occasionally sends closing letters to companies when they have investigated an alleged unfair or deceptive practice but have decided not to pursue an enforcement action.[173] This information can be quite helpful to companies as they could provide some indication as to which practices the FTC considered fair and truthful. The FTC should issue more of these letters, particularly with respect to privacy-related allegations of unfair practices, and the agency should provide more detail regarding its interpretation of Section 5 to the facts at issue.

One good example of a closing letter regarding data security is the agency's letter to Monster Worldwide, Inc. regarding a data security breach that resulted in the data of over a million customers who sought jobs using Monster's services being used in a targeted

---

[171] Jeff Sovern, Private Actions Under the Deceptive Trade Practices Acts: Reconsidering the Ftc Act As Rule Model, 52 Ohio St. L.J. 437, 441 (1991).

[172] Daniel J. Solove and Woodrow Hartzog, The FTC and the New Common Law of Privacy, 114 Colum. L. Rev. 583 (2014), available at http://ssrn.com/abstract=2312913.

[173] Staff Closing Letters, FTC.gov, http://www.ftc.gov/enforcement/cases-proceedings/closing-letters-and-other-public-statements/staff-closing-letters?title=&field_matter_number_value=&field_document_description=&date_filter[min]&date_filter[max]&page=1; Closing Letters and Other Public Statements, FTC.gov, http://www.ftc.gov/enforcement/cases-and-proceedings/closing-letters-and-other-public-statements.

phishing campaign.[174] The FTC did not file a complaint against Monster. According to the FTC, "Our investigation of Monster sought to determine if Monster engaged in unfair or deceptive acts or practices by failing to provide reasonable security for its customer contact information. The investigation focused on the risks raised by Monster's storage of this information and whether Monster acted reasonably in anticipating and addressing those risks."[175] In listing the reasons why the agency decided to close the investigation, it considered many factors including "the extent to which the risk at issue was reasonably foreseeable at the time of the compromise; the nature and magnitude of the risk relative to the other risks; the benefits relative to the costs of protecting against the risks; Monster's overall data security practices; the duration and scope of the compromise; the level of consumer injury; the type of information disclosed without authorization; and Monster's overall response to the incident."[176] The FTC stated that "[a]pplying these factors, the circumstances in this matter contrast with those in recent enforcement actions brought by the commission, many of which involved significant failures to address well-known vulnerabilities affecting inherently sensitive personal information such as Social Security numbers and credit card numbers."[177]

The FTC then offered more guidance for Monster and other companies dealing with personal information stating, "We continue to emphasize that data security is an ongoing process, and that as risks, technologies, and circumstances change over time, companies must adjust their information security programs accordingly. As noted above, the staff is concerned with the growing prevalence of personalized or targeting phishing attacks-attacks that may be facilitated by the failure to provide reasonable security for storehouses of customer contact information accessible for viewing and downloading online. Thus, we expect companies that house such data to take appropriate steps to protect it."[178]

The FTC then goes a step further to provide specific notice of what constitutes good security practices, stating, "Depending on the circumstances, such steps may include: avoiding the use of simple, easily guessed passwords or other credentials used by customers to access company data; implementing measures to ensure that those who access the company's online services using legitimate customer credentials are in fact authorized users of the system; and training customer service representatives to detect and defeat attempts to obtain customer credentials though social engineering or pretexting…Further, we expect such companies to remain vigilant in identifying new methods of attack by fraudsters and identify thieves and taking reasonable precautions to defend against such attacks."[179] Thus, in this one letter in 2008, the FTC has identified a threat to consumers and corresponding obligation to companies, explained why the FTC did not pursue an enforcement action against the company under investigation, and provided explicit steps for fair data security practices to be followed by all handling consumer data.

---

[174] Closing Letter to Timothy C. Blank, Dechert, LLP, FTC (March 6, 2008), http://www.ftc.gov/sites/default/files/documents/closing_letters/monster-worldwide-inc./monsterworldwide.pdf.
[175] *Id.*
[176] *Id.*
[177] *Id.*
[178] *Id.*
[179] *Id.*

In short, the FTC must become more transparent. Closing letters like the one issued to Monster are a great start. As we have argued in an earlier paper, the FTC is developing the functional equivalent of a common law of data protection. In order to do so effectively, it must provide information not just about why companies are in violation of Section 5 but also about why companies might not be. Having information about cases that are dropped is key to understanding the whole picture. In the common law, courts cannot make public only opinions granting summary judgment and not disclose opinions denying summary judgment.

Moreover, more flexibility should be exercised by the FTC in rewarding companies for the good things that they are doing. There are many dimensions in how companies engage in data protection, and the FTC often focuses on the shortcomings. But in many cases, the situation is not as binary as good or bad. Instead, there is often a mix of good and bad practices. Companies could do 99 out of 100 things right, and make one mistake, and violate Section 5. These mistakes should be penalized, but companies that do 0 out of 100 things right should be treated differently than those that do 99 out of 100 right. In its consent decrees, the FTC has not done enough to adjust the audit period or other measures to reward good practices when there is good mixed with bad.

One thing the FTC could do is seek milder punishments and shorter auditing periods from companies that did most things right and made a good faith attempt at compliance. While the FTC does not enter into a twenty-year consent orders with every company it files a privacy-related complaint against, this is the most common and burdensome duration of such agreements.[180] For some truly reckless organizations, this duration is likely justified. Yet for others that did many things right and other things wrong, a twenty-year consent order is overkill. The FTC might consider consent orders that last only a few years for companies that took significant steps to protect user data yet still ran afoul of Section 5. Moreover, shorter periods would free up FTC resources, hopefully enabling the FTC to increase the number of enforcement actions it brings.

More proportionate and milder penalties could have a number of positive effects. It would encourage risk-averse companies to engage in as many mitigating practices as possible to ensure that in the event a company is the subject of an FTC complaint the sting will be minimized. Yet it would still allow the FTC a great deal of flexibility in defining what practices are deceptive or unfair under Section 5 because merely engaging in some good data protection practices would not guarantee compliance with Section 5. Furthermore, the FTC might be incentivized to pursue a few more complaints in acknowledged grey areas for companies rather than just "slam dunk" cases. This would provide more guidance for companies at the margins and better reflect a true common law-like approach to data protection.

In cases where the FTC is operating more in a grey zone, the penalties would be less than in cases where there have been cases addressing the particular issue. Companies should be expected to follow the FTC's jurisprudence in the area much like they follow common law standards in areas relevant to their business. When those standards are clearly established, violations should be treated more harshly than when new standards are being recognized or developed.

[180] Solove & Hartzog, *supra* note ^.

If the FTC is going to take a bolder role, it should provide a little more leeway to companies at first. Where the FTC recognizes new standards or pushes the law forward in a more aggressive way, the FTC should have a "training wheels" style approach, being less punitive. After a reasonable time period, the training wheels should come off, and no leniency provided. But at the outset, if the FTC wants to evolve the law at a greater pace, it will likely go more smoothly under such an approach. This will also address concerns about fair notice that some critics raise and that are likely to become greater if the FTC exercises its power more robustly.

As we noted earlier, the FTC could use assistance from Congress to expand its jurisdiction to include non-commercial entities that are engaging in commercial practices. Moreover, rulemaking authority would be an essential tool for the FTC to develop more systematic rules where best suited, to increase the clarity of its guidance, and to more nimbly integrate mitigating factors into its analysis of how companies violating Section 5 should be treated. Ultimately, however, privacy and data security are complex issues that depend a lot on context. They cannot be readily reduced to a punch list and they involve a considerable amount of balancing of different values. Guidance and rules are always good, but there are limits to how complete and specific they can be for issues that are highly complex, dynamic, and contextual. This is why the case-by-case approach should remain a key feature of the system.

CONCLUSION

Despite a wave of criticism that the FTC's data protection enforcement is exceeding its powers, the FTC has, in fact, been well within the scope of its authority. There is significant room in the broad domain marked out by Section 5 of the FTC Act for the FTC to expand its enforcement and develop more progressive data protection standards. And the FTC should do so. Not only would expanded FTC involvement in this domain help protect consumers, but it will also help harmonize a fragmented and discordant data protection regulatory regime and make the U.S. approach more consistent with that of other countries, facilitating the exchange of data across borders. The FTC has great potential to regulate data protection with the appropriate nuance and focus.

The FTC was right to be conservative as it slowly began to regulate unfair and deceptive privacy-related practices. In the late 1990s when the FTC first starting bringing privacy-related complaints, it was unclear how privacy-related activities should be regulated and who should take the lead in doing so. But much has changed over the past two decades. An entire body of complaints has given shape to the FTC's broad mandate. A robust community of privacy professionals now exists to counsel companies of all sizes on their data protection obligations. New technologies like facial recognition and biometrics as well as new concepts like big data and digital market manipulation will continue to challenge policymakers.

Now is the right time for the FTC to move forward boldly. The FTC has robust powers, and it should be using them to a much greater degree, provided that the agency also becomes more transparent in its enforcement and more willing to use a mixture of carrots and sticks. It has the ability to develop the law of data protection in effective new ways. Over the past two decades, the FTC has slowly inched its way into a more central role in regulating data protection. It is now in the ideal position to take center stage and take U.S. data protection law to a new level.