The Scope and Potential of FTC Data Protection

Woodrow Hartzog and Daniel J. Solove***

Abstract

For more than fifteen years, the 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. Recently, the FTC's powers for data protection have been challenged by Wyndham Worldwide Corp. *and* LabMD. *These recent cases raise a fundamental issue, and one that has surprisingly not been well explored: How broad are the FTC's privacy and data security regulatory powers? How broad should they be?*

In this Article, we address the issue of the scope of FTC authority in the areas of 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 that its granted jurisdiction can 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 remedies available in tort or contract, or by various statutes. In contrast to the legal theories underlying these other claims of action, the FTC can regulate with a much different and more flexible understanding of harm than one focused on monetary or physical injury.

Thus far, the FTC has been quite modest in its enforcement, focusing on the most egregious offenders and enforcing the most widespread industry norms. Yet the FTC can and should push the development of norms a little more (though not in an extreme or aggressive way). We discuss steps the FTC should take to change the way it exercises its power, such as with greater transparency and more nuanced sanctioning and auditing.

---

* Associate Professor, Cumberland School of Law at Samford University; Affiliate Scholar, The Center for Internet and Society at Stanford Law School. The authors would like to thank Howard Beales, Danielle Citron, James Cooper, Chris Hoofnagle, Gus Hurwitz, William Kovacic, Geoff Manne, Mark McKenna, Maureen Ohlhausen, Paul Ohm, Lydia Parnes, Berin Szoka, Jay Tidmarsh, David Vladeck, Stephen Yelderman, the faculty at the University of Notre Dame Law School, participants of the Sixth Annual Privacy Law Scholars Conference, and the participants of the Research Roundtable on the Future of Privacy & Data Security Regulation hosted by the Law and Economics Center at George Mason University School of Law. The authors would like to thank the Law and Economics Center at George Mason University School of Law for its support of this research.

** John Marshall Harlan Research Professor of Law, The George Washington University Law School.

Table of Contents

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. Throughout most of this time, the FTC's power to regulate privacy and data security went unchallenged—until quite recently. In *FTC v. Wyndham Worldwide Corp.*,[1] a hotel chain challenged the FTC's au-

[1] FTC v. Wyndham Worldwide Corp., 10 F. Supp. 3d 602 (D.N.J. 2014), *aff'd*, 799 F.3d 236 (3d Cir. 2015).

thority to regulate data security practices.[2] In *LabMD, Inc.*,[3] a medical diagnostics company raised a similar challenge.[4]

These recent cases raise a fundamental issue, and one that has surprisingly not been well explored: How broad are the FTC's privacy and data security regulatory powers? How broad should they be?

In this Article, we address the scope of the FTC's authority over privacy and data security, two related areas that 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 that 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 U.S. 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 the FTC's 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 is broad because it emerges from Section 5 of the Federal Trade Commission Act of 1914 ("FTC Act"),[5] which has an intentionally broad scope.

Critics contend that the FTC is engaging in a form of rulemaking in this area where it lacks meaningful rulemaking authority. Worse still, the critics argue, the FTC is attempting to enforce these "rules" without articulating them clearly, and thus failing to provide adequate notice about them. We argue that any time 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 also argue that, contrary to the critics' contentions, the FTC has generally been quite clear and consistent in its approach. For ex-

---

2 *Id.* at 607; *see also* First Amended Complaint for Injunctive & Other Equitable Relief at 2, *Wyndham*, 10 F. Supp. 3d 602 (No. CV 12-1365-PHX-PGR) [hereinafter Wyndham Complaint]; Julie Sartain, *Analyzing* FTC v. Wyndham, Int'l Ass'n Privacy Professionals (Oct. 5, 2012), https://privacyassociation.org/news/a/2012-10-11-analyzing-ftc-vs.-wyndham/.

3 Complaint, LabMD, Inc., FTC File No. 102-3099, 2013 WL 5232775 (F.T.C. Aug. 28, 2013) [hereinafter LabMD Complaint].

4 *See* Respondent LabMD, Inc.'s Answer & Defenses to Admin. Complaint at 6, *LabMD, Inc.*, 2013 WL 5348553, at *3.

5 Federal Trade Commission (FTC) Act of 1914 § 5, 15 U.S.C. § 45 (2012).

ample, the FTC has based its data security jurisprudence on industry standards and a 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 nonincremental manner. The standards evolve in a common-law-like fashion, a developmental pattern typified by incremental change and 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.

Critics have also argued that the FTC's authority cannot overlap with that of other agencies, which it does in a number of instances. We contend that Section 5 will inevitably overlap with other statutes and regulatory domains, that the FTC routinely shares authority with other administrative agencies, and that such overlap is manageable.

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 linchpin in the U.S. data protection 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 has made the self-regulation significantly more meaningful through its enforcement of the promises companies make about the way they collect, use, and protect data. The FTC has filled gaps when a number of large industries have not been regulated by federal data protection statutes. In many instances, the FTC is the only regulator with the resources to enforce necessary protections like data security. Moreover, the FTC has played a pivotal role in promoting international confidence regarding privacy in the United States. Loss of FTC privacy jurisprudence would threaten the development of law designed to facilitate the international exchange of personal information, such as the former U.S.-E.U. Safe Harbor agreement.

We also 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 than those focused on monetary or physical

injury. According to the FTC, even incremental harms that affect a large group of consumers can be substantial.

Next, 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. 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. Po-

litical 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.[6]

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.[7] Under this statute, "unfair or deceptive acts or practices in or affecting commerce, are hereby declared unlawful."[8] The FTC began its foray into privacy and data security by focusing on promises companies voluntarily made in their privacy policies.[9] When companies later failed to live up to these promises, the FTC claimed that this was a deceptive trade practice.[10]

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 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

---

6 *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) (citing Fed. Trade Comm'n, Privacy Online: A Report to Congress i–ii (1998), https://www.ftc.gov/sites/default/files/documents/reports/privacy-online-report-congress/priv-23a.pdf; Fed. Trade Comm'n, Self-Regulation and Privacy Online: A Report to Congress 6 (1999), https://www.ftc.gov/system/files/documents/reports/self-regulation-privacy-onlinea-federal-trade-commission-report-congress/1999self-regulationreport.pdf) ("The FTC initially sought to deal with online privacy issues by encouraging industry self-regulation.").

7 Daniel J. Solove & Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, 114 Colum. L. Rev. 583, 598 (2014).

8 15 U.S.C. § 45(a)(1) (2012).

9 Solove & Hartzog, *supra* note 7, at 598–99.

10 *Id.* at 599.

did not rely only on explicit promises made.[11] The FTC soon uncoiled its power to police unfair trade practices and began bringing claims.[12]

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 ("HHS") is limited to regulating entities subject to the Health Insurance Portability and Accountability Act ("HIPAA"),[13] and countless industries do not fall under HIPAA.[14] Similarly, the Federal Communications Commission has jurisdiction over telecommunications, satellite, broadcast, and cable companies, but its range does not extend much further.[15]

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.[16] 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 that are unfair or deceptive.[17] 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 argued:

> The FTC's brief asserts a staggeringly broad theory of agency power. . . . The FTC believes that it can engage in

---

11 *Id.* at 628.

12 *Id.* at 638.

13 Health Insurance Portability and Accountability Act (HIPAA) of 1996 § 264(a), 42 U.S.C. § 1320d-2 (2012).

14 Solove & Hartzog, *supra* note 7, at 587 & n.7.

15 *See* 47 U.S.C. §§ 151–152 (2012); *What We Do*, FED. COMM. COMMISSION, http://www.fcc.gov/what-we-do (last visited Oct. 6, 2015) ("The Federal Communications Commission regulates interstate and international communications by radio, television, wire, satellite and cable . . . .").

16 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) (2012).

17 *See* H.R. REP. NO. 63-1142, at 19 (1914) (Conf. Rep.) (finding that, regarding unfairness, "[i]f Congress were to adopt the method of definition, it would undertake an endless task.").

> 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.[18]

Wyndham and others have faulted the FTC for enforcement in many areas also enforced by other agencies. For example, LabMD notes in its dispute with the FTC that LabMD is also subject to enforcement by HHS.[19] The FTC also enforces in areas regulated by other federal and state statutes, such as data-breach notification laws[20] 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 was 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, where the breaching parties used similar techniques in all three instances to access personal information stored on the Wyndham-branded hotels' property

---

18 Reply in Support of Motion to Dismiss by Defendant Wyndham Hotels & Resorts LLC at 1, FTC v. Wyndham Worldwide Corp., 10 F. Supp. 3d 602 (D.N.J. 2014) (No. CV 12-1365-PHX-PGR) [hereinafter Wyndham Reply in Support of Motion to Dismiss]; *see also* Proposed Brief of *Amici Curiae* Chamber of Commerce of the United States of America et al. in Support of Defendants at 5, *Wyndham*, 10 F. Supp. 3d 602 (No. 2:13-cv-01887-ES-SCM) [hereinafter Proposed Brief of Amici Curiae] ("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.").

19 *See* Order Denying Respondent LabMD's Motion to Dismiss at 3 n.4, LabMD, Inc., FTC Docket No. 9357, 2014 WL 253518 (F.T.C. Jan. 16, 2014); *see also* 42 U.S.C. § 1320d-5(e) (2012) (confirming power of HHS Office for Civil Rights to "use corrective action" against persons who fail to comply with HIPAA requirements).

20 Gerard M. Stegmaier & Wendell Bartnick, *Psychics, Russian Roulette, and Data Security: The FTC's Hidden Data-Security Requirements*, 20 GEO. MASON L. REV. 673, 673–76 (2013).

management system servers, including "customers' payment card account numbers, expiration dates, and security codes."[21]

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" its network.[22] According to the FTC, more than 619,000 consumers' payment card account numbers were compromised, and "[c]onsumers 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."[23]

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."[24] 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 [Wyndham] control[s] the Information, the Information is used only as authorized by [Wyndham] and consistent with [its] Policy, and that the Information is not improperly altered or destroyed."[25] The FTC alleged that Wyndham actually provided deficient data security practices contrary to their representations of following "industry standard practices."[26]

In addition to claiming deceptiveness, the FTC also attacked Wyndham's data security practices on fairness grounds.[27] Specifically, the FTC identified practices that "unreasonably and unnecessarily exposed consumers' personal data to unauthorized access and theft."[28] 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, and failed to remedy known security vulnerabili-

21 Wyndham Complaint, *supra* note 2, at 12–13.

22 *Id.* at 13.

23 *Id.* at 18.

24 *See id.* at 8–10.

25 *Id.* at 9–10.

26 *See id.* at 2, 9.

27 *Id.* at 19.

28 *Id.* at 10.

ties (for example by connecting insecure servers with outdated operating systems ("OS") unable to get security patches).[29] 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, failed to employ reasonable measures to detect and prevent unauthorized access, failed to follow proper incident response procedures, including monitoring for malware postbreach, and failed to adequately restrict third-party vendor access.[30]

Unlike nearly all other defendants in FTC actions,[31] Wyndham did not settle with the FTC. Instead, the FTC brought an action in federal court.[32] On April 7, 2014, the United States District Court for the District of New Jersey issued its long-awaited opinion in the case.[33] 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.[34] 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.[35] The Third Circuit Court of Appeals affirmed the district court's rejection of Wyndham's arguments.[36]

Wyndham made three principal arguments related to the scope of the FTC's unfairness authority in its April 26, 2013 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.[37] U.S. District Judge Salas resolved each of these issues in favor of the FTC and denied Wyndham's motion to dismiss.[38]

Regarding the scope of the FTC's Section 5 authority, Wyndham asserted that the "overall statutory landscape" made it clear that un-

---

29 *Id.* at 10–12.

30 *Id.*

31 *See* Solove & Hartzog, *supra* note 7, at 606–07.

32 *See* FTC v. Wyndham Worldwide Corp., 10 F. Supp. 3d 602, 609 (D.N.J. 2014).

33 *Id.* at 602.

34 *Id.* at 612.

35 *Id.* at 617.

36 FTC v. Wyndham Worldwide Corp., 799 F.3d 236 (3d Cir. 2015).

37 Motion to Dismiss by Defendant Wyndham Hotels & Resorts LLC at 7, 14, 19, *Wyndham*, 10 F. Supp. 3d 602 (No. 2:13-cv-01887-ES-SCM) [hereinafter Wyndham Motion to Dismiss].

38 *Wyndham*, 10 F. Supp. 3d at 631.

fairness authority does not extend to data security.[39] 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.[40] Relying on an analogous case, *FDA v. Brown & Williamson Tobacco Corp.*,[41] Wyndham argued that these targeted data security statutes indicated that the FTC lacked broader authority to regulate in this area.[42]

Wyndham also argued that, like the Food and Drug Administration ("FDA") in *Brown & Williamson*, the FTC explicitly disclaimed authority to regulate data security under Section 5's unfairness prong.[43] Judge Salas, however, rejected the comparison: "[T]he Court is not convinced that [prior FTC] 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."[44] The court noted that the FTC actually "brought unfairness claims in the data-security context shortly after these representations. And the FTC's subsequent representations confirm its authority in this arena, not deny it."[45]

On appeal, the Third Circuit also rejected Wyndham's argument that because Congress enacted data security laws to regulate specific industries, Congress did not intend for the FTC to be able to regulate data security under the FTC Act.[46] The court held that the FTC has the power to regulate data security through Section 5.[47] The court examined several statutes granting the FTC authority to regulate data security and distinguished the powers granted in these statutes from the powers the FTC has under Section 5.[48]

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."[49] The company also argued that the FTC failed to articulate exactly

---

39 *Id.* at 611.

40 *Id.* at 611 & n.4.

41 FDA v. Brown & Williamson Tobacco Corp., 529 U.S. 120 (2000).

42 *Wyndham*, 10 F. Supp. 3d at 611.

43 *Id.* at 614.

44 *Id.*

45 *Id.* (citation omitted).

46 FTC v. Wyndham Worldwide Corp., 799 F.3d 236, 247–48 (3d Cir. 2015).

47 *Id.*

48 *Id.* at 248.

49 Wyndham Reply in Support of Motion to Dismiss, *supra* note 18, at 7.

what the vague standards created by use of the terms "reasonable," "adequate," or "proper" require.[50]

The FTC disagreed with Wyndham's argument that rulemaking is the only proper way for the FTC to regulate data security.[51] According to the FTC, rulemaking would be inappropriate because data security is highly contextual and always changing.[52] Regarding the definition of "reasonable" security, 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."[53]

The FTC also asserted "data-security standards can be enforced in an industry-specific, case-by-case manner," analogizing its strategy in regulating data security with the approach of other agencies that bring actions without "particularized prohibitions" such as the National Labor Relations Board ("NLRB") and the Occupational Safety and Health Act ("OSHA").[54]

The Third Circuit took up the fair notice challenge by Wyndham on due process grounds. Under the Due Process Clause of the U.S. Constitution, due process is violated if regulation "fails to provide a person of ordinary intelligence fair notice of what is prohibited, or is so standardless that it authorizes or encourages seriously discriminatory enforcement."[55] The Third Circuit noted that the standard is "especially lax for civil statutes that regulate economic activities. For those statutes, a party lacks fair notice when the relevant standard is 'so vague as to be no rule or standard at all.'"[56] The Third Circuit concluded:

> We thus conclude that Wyndham was not entitled to know with ascertainable certainty the FTC's interpretation of what cybersecurity practices are required by § 45(a). Instead, the relevant question in this appeal is whether Wyndham had fair notice that its conduct could fall within the

50 *Id.* at 9.

51 Plaintiff's Response in Opposition to Wyndham Hotels & Resorts' Motion to Dismiss at 11–13, *Wyndham*, 10 F. Supp. 3d 602 (No. 2:12-cv-01365-PHX-PGR).

52 *Id.* at 12.

53 *Wyndham*, 10 F. Supp. 3d at 616–17.

54 *Id.* at 617.

55 FTC v. Wyndham Worldwide Corp., 799 F.3d 236, 249 (3d Cir. 2015) (quoting FCC v. Fox Television Stations, Inc., 132 S. Ct. 2307, 2317 (2012)).

56 *Id.* at 250 (quoting CMR D.N. Corp. v. City of Phila., 703 F.3d 612, 631–32 (3d Cir. 2013)).

> meaning of the statute. If later proceedings in this case develop such that the proper resolution is to defer to an agency interpretation that gives rise to Wyndham's liability, we leave to that time a fuller exploration of the level of notice required. For now, however, it is enough to say that we accept Wyndham's forceful contention that we are interpreting the FTC Act (as the District Court did). As a necessary consequence, Wyndham is only entitled to notice of the meaning of the statute and not to the agency's interpretation of the statute.[57]

The court went on to note that although "there will be borderline cases where it is unclear if a particular company's conduct falls below the requisite legal threshold," due process does not require laser-sharp precision: "But under a due process analysis a company is not entitled to such precision as would eliminate all close calls. Fair notice is satisfied here as long as the company can reasonably foresee that a court could construe its conduct as falling within the meaning of the statute."[58]

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.[59] Wyndham also contended that "incidental injuries that consumers suffered" such as the cost of remedial finance monitoring were insufficient to constitute a "substantial injury."[60] 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.[61] This issue was not resolved by the district court.[62]

The Third Circuit rejected Wyndham's argument that the FTC failed to establish "substantial injury to consumers" as required to enforce unfairness. It wrote:

> Although unfairness claims "usually involve actual and completed harms, they may also be brought on the basis of likely rather than actual injury." And the FTC Act expressly contemplates the possibility that conduct can be unfair before actual injury occurs. More importantly, that a company's

57 *Id.* at 255.

58 *Id.* at 256.

59 *Wyndham*, 10 F. Supp. 3d at 621–22, 625.

60 *Id.* at 622.

61 *Id.* at 623 n.15.

62 *Id.*

> conduct was not the most proximate cause of an injury generally does not immunize liability from foreseeable harms.[63]

On the heels of Wyndham, another defendant challenged the FTC's Section 5 enforcement authority in an FTC Adjudicative Proceeding. 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."[64] In a press release, the FTC described its complaint as alleging "that in two separate incidents, LabMD collectively exposed the personal information of approximately 10,000 consumers."[65] 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."[66] The FTC claimed that this failure to "employ reasonable and appropriate measures to prevent unauthorized access to personal information, including dates of birth, SSNs, medical test codes, and health information," was an unfair practice.[67]

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.[68] 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.[69]

Although *Wyndham* and *LabMD* involved data security issues, the import of their arguments extends 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 de-

---

63 *Wyndham*, 799 F.3d at 246 (citations omitted).

64 Press Release, Fed. Trade Comm'n, FTC Files Complaint Against LabMD for Failing to Protect Consumers' Privacy (Aug. 29, 2013), http://www.ftc.gov/news-events/press-releases/2013/08/ftc-files-complaint-against-labmd-failing-protect-consumers; *see also* LabMD Complaint, *supra* note 3.

65 *Id.*

66 *Id.*

67 LabMD Complaint, *supra* note 3, at 5.

68 *See* Order Denying Respondent LabMD's Motion to Dismiss, *supra* note 19, at 1, 14.

69 *Id.* at 12.

veloping 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.[70]

Similarly, Berin Szoka and Geoffrey 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 develop[ed] 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.[71]

In an amicus brief filed in *Wyndham*, TechFreedom, the International Center for Law & Economics, Berin Szoka, Geoffrey Manne, and several other scholars including Gus Hurwitz, Todd Zywicki, and Paul Rubin argued 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."[72]

Gerard 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 pronouncements raise equitable considerations that create serious due process concerns."[73] The authors ask, "[i]f an entity cannot ascertain what the law is, how

---

70 Scott, *supra* note 6, at 183 (footnote omitted).

71 Berin Szoka & Geoffrey Manne, *The Second Century of the Federal Trade Commission*, TECHDIRT (Sept. 26, 2013, 8:05 PM), http://www.techdirt.com/blog/innovation/articles/20130926/16542624670/second-century-federal-trade-commission.shtml.

72 Amici Curiae Brief of TechFreedom, Int'l Ctr. for Law & Econ. & Consumer Prot. Scholars at 7, FTC v. Wyndham Worldwide Corp., 10 F. Supp. 3d 602 (D.N.J. 2014) (No. 2:13-cv-01887(ES)(SCM)) [hereinafter Wyndham Amicus Brief], http://docs.techfreedom.org/Wyndham_Amici_Brief.pdf; *see also* Justin (Gus) Hurwitz, *Data Security and the FTC's UnCommon Law*, IOWA L. REV. (forthcoming 2015) (draft version available at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2574257##).

73 Stegmaier & Bartnick, *supra* note 20, at 676.

can it know what it must do—especially where liability most commonly arises out of the malfeasance of others?"[74]

Other critics assail the FTC for taking action 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."[75]

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.[76]

Similarly, 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 [Federal Communications Commission], local taxicab commissions or European-style data protection agencies.[77]

To Szoka and Manne, while the case-by-case approach is good in theory, they still contend that "how the agency works is deeply prob-

---

74 *Id.*

75 James C. Cooper, *Identity Theft, Not Big Data, Should Be at the Top of the FTC's Priority List*, DAILY CALLER (Sept. 24, 2013, 5:38 PM), http://dailycaller.com/2013/09/24/identity-theft-not-big-data-should-be-at-the-top-of-the-ftcs-priority-list/2.

76 *Szoka Statement on Facebook FTC Privacy Settlement*, TECHFREEDOM (Nov. 29, 2011), http://techfreedom.org/post/58365342326/szoka-statement-on-facebook-ftc-privacy.

77 *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.

lematic."[78] They 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."[79] 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.[80] 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

Contrary to the arguments of 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 District Court Judge Salas in *Wyndham*, the concepts of deceptiveness and unfairness in the FTC Act are intentionally defined at an extremely broad level.[81] 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 practices that are unfair—with virtually no hard boundary lines.[82] 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,[83] but this argument is misplaced. Even in light of the limitations imposed by Congress[84] in response to the

---

78 *Id.*

79 *Id.*

80 For example, the FTC has wide discretion as to which actor the FTC may file a complaint against and is not required to pursue worst actors or any actor in particular. *See* Moog Indus., Inc. v. FTC, 355 U.S. 411, 413–14 (1958) (per curiam).

81 FTC v. Wyndham Worldwide Corp., 10 F. Supp. 3d 602, 615 (D.N.J. 2014).

82 *See* FTC v. Sperry & Hutchinson Co., 405 U.S. 233, 239–44 (1972).

83 *E.g.*, Proposed Brief of Amici Curiae, *supra* note 18, at 3 ("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.").

84 *See* Federal Trade Commission Act Amendments of 1994, Pub. L. No. 103-312, § 9, 108 Stat. 1691, 1695 (codified at 15 U.S.C. § 45(n) (2012)).

FTC's earlier broad statements on deception and unfairness,[85] the FTC's authority remains explicitly general and expansive.[86]

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.[87] 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.[88] Although the requirement that a deception be "material" to consumers[89] 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.[90]

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 now much broader.

The FTC's unfairness authority is also comprehensive. According to the FTC, "[t]he present understanding of the unfairness standard is the result of an evolutionary process. The statute was deliberately framed in general terms since Congress recognized the impossibility of drafting a complete list of unfair trade practices that would not quickly become outdated or leave loopholes for easy evasion."[91] Notably, the FTC can find a practice unfair even when it is otherwise legally permissible.[92]

Regarding the meaning of unfairness, the House Conference Report famously stated:

---

85 FED. TRADE COMM'N, COMMISSION STATEMENT OF POLICY ON THE SCOPE OF THE CONSUMER UNFAIRNESS JURISDICTION (1980), *reprinted in* Int'l Harvester Co., 104 F.T.C. 949, 1072–88 (1984) [hereinafter cited as UNFAIRNESS STATEMENT with page references to *Int'l Harvester Co.*]; Letter from James C. Miller III, Chairman, Fed. Trade Comm'n, to John D. Dingell, Chairman, Comm. on Energy & Commerce (Oct. 14, 1983), *reprinted in* Cliffdale Assocs., Inc., 103 F.T.C. 110, 175–98 (1984) [hereinafter cited as DECEPTION STATEMENT with page references to *Cliffdale Associates*].

86 *See* UNFAIRNESS STATEMENT, *supra* note 85, at 1067–68; 15 U.S.C. § 45(a)(2) (2012).

87 *See* DECEPTION STATEMENT, *supra* note 85 at 183.

88 Solove & Hartzog, *supra* note 7, at 628–38.

89 FTC v. Wyndham Worldwide Corp., 10 F. Supp. 3d 602, 628 (D.N.J. 2014).

90 *See* Solove & Hartzog, *supra* note 7, at 628–29 (collecting cases).

91 Int'l Harvester, 104 F.T.C. at 1072 (FTC Policy Statement on Unfairness); *see* 15 U.S.C. § 45(n) (providing that the FTC may consider established public policies in determining whether an act of practice is unfair).

92 Spiegel, Inc. v. FTC, 540 F.2d 287, 292 (7th Cir. 1976) (citing FTC v. Sperry & Hutchison, Co., 405 U.S. 233, 244 (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.").

> It is impossible to frame definitions which 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.[93]

Thus, it is the FTC that is responsible, subject to judicial review, for identifying unfair trade practices.[94]

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.[95] The Court stated 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.'"[96] 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.[97]

The opinions in *Wyndham* support this view. Judge Salas rejected Wyndham's argument that the FTC does not have the authority to regulate data security.[98] 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 in-

---

93 H.R. REP. NO. 63-1142, at 19 (1914) (Conf. Rep.).

94 *See id.*

95 UNFAIRNESS STATEMENT, *supra* note 85, at 1072 (citing FTC v. Raladam Co., 283 U.S. 643, 648 (1931)); 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.")).

96 *Raladam Co.*, 283 U.S. at 648 (quoting Davidson v. New Orleans, 96 U.S. 97, 104 (1878)).

97 FTC v. Standard Educ. Soc'y, 86 F.2d 692, 696 (2d 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 KINTNER & WILLIAM KRATZKE, FEDERAL ANTITRUST LAW 89–90 ("[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 which the Commission cannot ever overstep, notwithstanding the increasing deference to agency interpretative skills." (footnote omitted)).

98 FTC v. Wyndham Worldwide Corp., 10 F. Supp. 3d 602, 612 (D.N.J. 2014).

jury 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.[99]

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 and thus would 'plainly *contradict* congressional policy.'"[100] 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 the tobacco products at issue in *Brown & Williamson*, as was argued by Wyndham.[101]

In an order denying LabMD's motion to dismiss, Commissioner Joshua Wright, writing for a unanimous Commission, confirmed the FTC's authority to enforce the FTC Act by adjudicating whether data security practices are unfair.[102] 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.'"[103] Citing a D.C. Circuit case, 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.'"[104] It observed that:

> The 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.[105]

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

---

99 *See id.* at 612–13.

100 *Id.* at 612 (quoting FDA v. Brown & Williamson Tobacco Corp., 529 U.S. 120, 139 (2000)).

101 *Id.* at 612–13.

102 Order Denying Respondent LabMD's Motion to Dismiss, *supra* note 19, at 1–2.

103 *Id.* at 5.

104 *Id.* (quoting Am. Fin. Servs. Ass'n v. FTC, 767 F.2d 957, 966 (D.C. Cir. 1985)).

105 *Id.*

actual unavoidable harm or likelihood thereof, which is not outweighed by countervailing benefits to consumers or competition.[106]

An exceptionally wide range of activities has been included in the FTC's unfairness and regulatory efforts, including creating a physical danger to children,[107] high pressure sales environments,[108] the unilateral imposition of fees in breach of a service contract,[109] and failure to disclose substantial risk of physical injury from hazardous exercise equipment.[110] Stephen Calkins stated, "[m]odern 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 practices."[111] Many of the alleged unfair actions seek to take advantage of vulnerable consumers, making exploitation the locus of many unfairness allegations.[112]

Thus, commentators, the Commission, the courts, and even Congress itself have repeatedly confirmed that 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.

---

106 15 U.S.C. § 45(n) (2012); *see also* Order Denying Respondent LabMD's Motion to Dismiss, *supra* note 19, at 5.

107 *See* Philip Morris, Inc., 82 F.T.C. 16, 19 (1973) (consent order) (requiring respondent to cease distributing free-sample razor blades in such a way that they could come into the hands of small children).

108 *See* Holland Furnace Co. v. FTC, 295 F.2d 302, 303–05 (7th Cir. 1961) (upholding Commission's cease and desist order when seller's servicemen dismantled home furnaces and then refused to reassemble them until the consumers had agreed to buy services or replacement parts).

109 *See* Orkin Exterminating Co. v. FTC, 849 F.2d 1354, 1355–56 (11th Cir. 1988) (upholding Commission cease and desist order when company unilaterally breached "over 200,000 contracts with its customers").

110 *See* Consumer Direct Inc., 113 F.T.C. 923, 928 (1990) (consent order); *FTC Charges Fitness Quest, Inc. with Making Deceptive Claims and Failing to Disclose a Safety Risk from Use of Its "Gut Buster" Exercise Device*, CASEWATCH (Aug. 27, 2006), http://www.casewatch.org/ftc/news/1990/gutbust.shtml.

111 Stephen Calkins, *FTC Unfairness: An Essay*, 46 WAYNE L. REV. 1935, 1962 (2000).

112 *See, e.g.*, FTC v. R.F. Keppel & Bro., 291 U.S. 304, 313–14 (1934) (finding unfairness where an action "exploit[s] consumers, children, who are unable to protect themselves"); Unfair or Deceptive Advertising and Labeling of Cigarettes in Relation to the Health Hazards of Smoking, 29 Fed. Reg. 8324, 8354–55 (July 2, 1964), *quoted in* FTC v. Sperry & Hutchinson Co., 405 U.S. 233, 244 n.5 (1972).

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.[113] 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.[114] The Fair Credit Reporting Act of 1970 ("FCRA")[115] already gave the FTC the authority to regulate the credit reporting industry.[116] New data protection laws and regulation began to emerge after the FTC started applying Section 5 to data protection in the mid-1990s.[117] For example, the privacy requirements of the Administrative Simplification rules of Title II of HIPAA went into effect in 2001, with compliance required as of 2003.[118] The Health Information Technology for Economic and Clinical Health Act of 2009 ("HITECH Act")[119] added a data breach notification requirement to HIPAA.[120] 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 active in the area.[121] It is important to note that when Congress passed HIPAA and later on when it passed the HITECH Act amending

113 *See, e.g.*, FTC v. Ken Roberts Co., 276 F.3d 583, 584 (D.C. Cir. 2001) ("The appellants claimed that, because the regulation of their advertising practices was subject to the exclusive jurisdiction of the Commodities Futures Trading Commission ("CFTC") or the Securities and Exchange Commission ("SEC"), the FTC lacked authority to investigate.").

114 Solove & Hartzog, *supra* note 7, at 590–94.

115 Fair Credit Reporting Act (FCRA), Pub. L. No. 91-508, §§ 601–22, 84 Stat. 1114, 1128–36 (1970) (codified as amended at 15 U.S.C. §§ 1681–1681x).

116 *Id.* § 621(a), 84 Stat. at 1134–35.

117 Solove & Hartzog, *supra* note 7, at 598–99.

118 *See* Standards for Privacy of Individually Identifiable Health Information, 65 Fed. Reg. 82,462, 82,462, 82,787 (Dec. 28, 2000) (codified at 45 C.F.R. pts. 160, 164); *HIPAA Administrative Simplification Statute and Rules*, U.S. DEP'T HEALTH & HUM. SERVS., http://www.hhs.gov/ocr/privacy/hipaa/administrative/ (last visited Oct. 6, 2015).

119 Health Information Technology for Economic and Clinical Health (HITECH) Act of 2009, Pub. L. No. 111-5, §§ 13001–13424, 123 Stat. 115, 226–79 (codified in scattered sections of 42 U.S.C.).

120 *Id.* § 13402, 123 Stat. at 260; *see* 45 C.F.R. §§ 164.400–.414 (2014).

121 *See supra* text accompanying notes 117–20.

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.[122]

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 of 1998 ("COPPA")[123] gave the FTC direct authority to enforce the statute's mandates for websites directed to children under thirteen.[124] Under COPPA, the FTC was also granted rulemaking authority, which it lacked for the most part under Section 5.[125] The Gramm-Leach-Bliley Act ("GLBA")[126] gave the FTC direct authority over data protection in the financial services industry.[127] 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.[128] 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?

---

122 42 U.S.C. § 17934(a), (c) (2012).

123 Children's Online Privacy Protection Act (COPPA), 15 U.S.C. §§ 6501–6505 (2012).

124 *Id.* §§ 6501(1), 6505(a).

125 *Id.* § 6505(d).

126 Gramm-Leach-Bliley Act, Pub. L. No. 106-102, 113 Stat. 1338 (1999) (codified in scattered sections of 12, 15 U.S.C.).

127 *Id.* §§ 504, 505, 522, 113 Stat. at 1439–41, 1447–48.

128 *Id.* § 504, 113 Stat. at 1439.

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.[129] As discussed above, Wyndham claimed 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.[130]

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 or 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.[131]

The FTC was created to have intentionally general and expansive jurisdiction.[132] 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.[133] 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."[134] 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.[135]

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 jurisdiction, one court has stated, "[b]ecause we live in 'an age of overlapping and concurring regulatory jurisdiction,' a court must proceed with the utmost caution before concluding that one agency may

---

129 *See* Wyndham Motion to Dismiss, *supra* note 37, at 1.

130 FTC v. Wyndham Worldwide Corp., 10 F. Supp. 3d 602, 611 & n.4 (D.N.J. 2014).

131 Solove & Hartzog, *supra* note 7, at 602–04 (discussing "expansion" of FTC's privacy jurisdiction).

132 *See supra* Part I.B.1.

133 15 U.S.C. §§ 13c, 45(a)(2) (2012). Nonprofit entities are ostensibly not engaged in "commerce."

134 Order Denying Respondent LabMD's Motion to Dismiss, *supra* note 19, at 12.

135 *Id.* (citing 15 U.S.C. § 45(a)(2)).

not regulate merely because another may."[136] Indeed, concurring and overlapping jurisdiction between administrative agencies and between agencies and statutes is not only common, but is often desirable.[137] 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."[138]

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.[139] For example, the FTC has worked with the FDA for over forty years regarding certain kinds of advertising for food and drugs.[140] Additionally, in examining FTC's deceptive advertising overlap with the Commodities Exchange Act and Investment Advisors Act ("IAA"), one court stated, "[t]he 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

136 FTC v. Ken Roberts Co., 276 F.3d 583, 593 (D.C. Cir. 2001) (citation omitted) (quoting Thompson Med. Co. v. FTC, 791 F.2d 189, 192 (D.C. Cir. 1986)); *see also* FTC v. Cement Inst., 333 U.S. 683, 694–95 (1948) ("We find nothing to justify a holding that the filing of a Sherman Act suit by the Attorney General requires the termination of these Federal Trade Commission proceedings."); FTC v. Texaco, Inc., 555 F.2d 862, 881 (D.C. Cir. 1977) ("It therefore appears that a court should approach gingerly a claim that one agency has conclusively determined an issue later analyzed from another perspective by an agency with different substantive jurisdiction.").

137 *See* Jacob E. Gersen, *Overlapping and Underlapping Jurisdiction in Administrative Law*, 2006 SUP. CT. REV. 201, 208 ("[S]tatutes that parcel out authority or jurisdiction to multiple agencies may be the norm, rather than an exception."); *id.* at 203 ("Because overlapping and underlapping jurisdictional assignment can produce desirable incentives for administrative agencies, statutes of this sort are useful tools for managing principal-agent problems inherent in delegation.").

138 *Id.* at 212.

139 *See, e.g.*, *Ken Roberts Co.*, 276 F.3d at 593.

140 *See* Memorandum of Understanding Between the Federal Trade Commission and the Food and Drug Administration, 36 Fed. Reg. 18,539, 18,539 (Sept. 16, 1971); Thompson Med. Co. v. FTC, 791 F.2d 189, 192 (D.C. Cir. 1986) ("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.").

duty of this court 'to regard each as effective'—at least absent clear congressional intent to the contrary."[141]

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.[142] For example, almost half of the FTC complaints alleging violations of COPPA also contained an allegation of deceptive trade practices, a Section 5 violation.[143] Almost all of the FTC complaints alleging violations of the GLBA also contained an allegation of deceptive or unfair trade practices.[144] These practices have not re-

---

141 *Ken Roberts Co.*, 276 F.3d at 593 (quoting Morton v. Mancari, 417 U.S. 535, 551 (1974)).

142 Solove & Hartzog, *supra* note 7, at 643.

143 *See* Complaint for Civil Penalties, Permanent Injunction, & Other Relief at 2, United States v. Path, Inc., No. 3:13-cv-00448-RS (N.D. Cal. Feb. 8, 2013); Complaint for Civil Penalties, Permanent Injunction, & Other Equitable Relief at 13, United States v. Artist Arena LLC, No. 1:12-cv-07386-JGK (S.D.N.Y. Oct. 3, 2012); Complaint for Civil Penalties, Permanent Injunction, & Other Equitable Relief at 1–2, United States v. Rockyou, Inc., No. 3:12-cv-1487-SI, (N.D. Cal. Mar. 27, 2012); Complaint for Civil Penalties, Injunctive, & Other Relief at 4, United States v. Godwin, No. 1:11-cv-3846-JOF (N.D. Ga. Feb. 1, 2012); Complaint for Civil Penalties, Injunction, & Other Relief at 4, United States v. Playdom, Inc., No. SACV11-0724-AG(ANx) (C.D. Cal. May 24, 2011); Complaint for Civil Penalties, Injunction, & Other Relief at 1, 7–8, United States v. Iconix Brand Grp., Inc., Case 09 Civ. 8864 (MGC) (S.D.N.Y. Nov. 5, 2009); Complaint for Civil Penalties, Injunctive, & Other Relief at 1, 5–6, United States v. Am. Pop Corn Co., No. C02-4008DEO (N.D. Iowa Feb. 14, 2002); Complaint for Civil Penalties, Injunctive, & Other Relief at 7–9, United States v. Lisa Frank, Inc., No. 01-1516-A (E.D. Va. Oct. 2, 2001); Complaint for Civil Penalties, Injunctive, & Other Relief at 8–10, United States v. Bigmailbox.com, Inc., No. 01-605-A (E.D. Va. Apr. 19, 2001); First Amended Complaint for Permanent Injunction & Other Equitable Relief, FTC v. Toysmart.com, LLC, No. 00-11341-RGS (D. Mass. July 21, 2000). It is not always clear if the FTC is alleging a violation of COPPA, a violation of Section 5, or both. For example, in *United States v. W3 Innovations, LLC*, No. 5:11-cv-03958-PSG (N.D. Cal. Sept. 8, 2011), 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. *See* Complaint for Civil Penalties, Permanent Injunction, & Other Equitable Relief at 1–2, 7, *W3 Innovations*, No. 5:11-cv-03958-PSG; *see also* Complaint for Civil Penalties, Injunction, & Other Relief at 2, 8, United States v. Industrious Kid, Inc., CV No. 08-0639 (N.D. Cal. Mar. 6, 2008) (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"); Complaint at 9, United States v. Xanga.com, Inc., No. 06 Civ. 6853 (SHS) (S.D.N.Y. Sept. 11, 2006) (same).

Contrast this with other FTC complaints where both the COPPA rule and Section 5 were alleged to have been violated. *See, e.g.*, Complaint for Complaint for Civil Penalties, Injunction, & Other Relief at 9–10, *Playdom*, No. SACV 11-0724-AG(ANx) (alleging violations of COPPA and Section 5 of the FTC Act independent of COPPA violation).

144 *See* Complaint for Permanent Injunction & Other Equitable Relief at 10–11, FTC v. Sun Spectrum Commc'ns Org., Inc., No. 03-8110 (S.D. Fla. Oct. 3, 2005), http://www.ftc.gov/os/caselist/0323032/031202cmp0323032.pdf; Complaint for Injunctive & Other Equitable Relief at 12–19, FTC v. Corp. Mktg. Sols., Inc., No. CIV-02 1256 PHX RCB (D. Ariz. July 18, 2002), http://www.ftc.gov/os/2002/07/cmscmp.pdf; First Amended Complaint for Injunctive & Other Equitable Relief at 6, FTC v. Garrett, Civil Action No.: H-01-1255 (S.D. Tex. Mar. 8, 2002), http://ftc.gov/os/2002/03/discreetdatacmplnt.pdf; Complaint for Injunctive & Other Equitable Relief at

sulted 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 the HITECH Act of 2009, where Congress directly addressed HHS's enforcement power and could have limited that power exclusively to HHS.[145] Interestingly, Congress chose to allow for *more* entities to enforce by authorizing state attorneys general to enforce HIPAA.[146]

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.[147] Moreover, as we noted in a previous work, the data security standards that the FTC has developed are quite consistent with those in the HIPAA Security Rule.[148]

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.[149] The FTC's enforcement of promises made in privacy policies in many ways overlaps the law of contract and promissory estoppel, although FTC enforcement has proven to be much more effective than these doctrines.[150]

56, FTC v. Guzzetta, No. 01-2335(DGT) (E.D.N.Y. Feb. 25, 2002), http://www.ftc.gov/os/2001/04/pretextingsmartdatacomplaint.pdf; Complaint at 3, Franklin's Budget Car Sales, Inc., FTC File No. 102-3094(Oct. 3, 2012), http://www.ftc.gov/os/caselist/1023094/121026franklinautomallcmpt.pdf; Complaint at 5, Premier Capital Lending, Inc., FTC File No. 072-3004 (Dec. 10, 2008) [hereinafter Premier Capital Lending Complaint], http://www.ftc.gov/os/caselist/0723004/081206pclcmpt.pdf; Complaint at 3–4, Goal Fin., LLC, FTC File No. 072-3013 (Apr. 9, 2008), http://www.ftc.gov/os/caselist/0723013/080415complaint.pdf; Complaint at 4–5, Nations Title Agency, Inc. FTC File No. 052-3117 (June 19, 2006) [hereinafter Nations Title Agency Complaint], http://www.ftc.gov/os/caselist/0523117/0523117NationsTitle_Complaint.pdf; Complaint at 2–3, Superior Mortg. Corp., FTC File No. 052-3136 (Dec. 14, 2005), http://www.ftc.gov/os/caselist/0523136/051216comp0523136.pdf.

145 *See supra* notes 119–22 and accompanying text.

146 *See* 42 U.S.C. § 1320d-5(d) (2012); *Health Information Privacy: State Attorneys General*, U.S. DEP'T HEALTH & HUM. SERVS., http://www.hhs.gov/ocr/privacy/hipaa/enforcement/sag/ (last visited Oct. 7, 2015).

147 *See* Modifications to the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules Under the Health Information Technology for Economic and Clinical Health Act and the Genetic Information Nondiscrimination Act, 78 Fed. Reg. 5566, 5579 (Jan. 25, 2013) (to be codified at 45 C.F.R. pts. 160, 164).

148 Solove & Hartzog, *supra* note 7, at 651–55.

149 *Compare id.* at 599 ("An 'unfair or deceptive' act or practice is a material 'representation, omission or practice that is likely to mislead the consumer acting reasonably in the circumstances, to the consumer's detriment.'"), *with* RESTATEMENT (SECOND) OF TORTS § 525 (AM. LAW INST. 1977) (defining fraudulent misrepresentation as a "misrepresentation of fact, opinion, intention or law for the purpose of inducing another to act or to refrain from action in reliance upon it").

150 Solove & Hartzog, *supra* note 7, at 589, 596–97.

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 U.S. approach to data protection is to have a series of different laws to regulate different corners of the economy.[151] 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.[152] And these borders would have to be adjusted with each new law that creates potential overlap.[153] 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.[154]

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.[155] They contend that the FTC simply waits until after a data breach occurs and then announces new data security rules and standards that the companies suffering the

---

151 *See id.* at 587.

152 *See* Gersen, *supra* note 137, at 210–11 (describing problems inherent in congressional grants of "overlapping" jurisdiction).

153 *See id.* at 208.

154 *See* Solove & Hartzog, *supra* note 7, at 676 (arguing that FTC has "created a body of common law doctrines").

155 *See* Wyndham Motion to Dismiss, *supra* note 37, at 10–11; Wyndham Amicus Brief, *supra* note 72, at 7–9; Proposed Brief of Amici Curiae, *supra* note 18, at 10–12; Respondent LabMD, Inc.'s Motion to Dismiss Complaint with Prejudice & to Stay Admin. Proceedings at 22–28, LabMD, Inc., FTC Docket No. 9357 (F.T.C. Aug. 28, 2013), https://www.ftc.gov/sites/default/files/documents/cases/131112respondlabmdmodiscomplaintdatyadminproceed.pdf; Gerard M. Stegmaier & Wendell Bartnick, *Another Round in the Chamber: FTC Data Security Requirements and the Fair Notice Doctrine*, J. INTERNET L., Nov. 2013, 1, 18–19; Scott, *supra* note 6, at 170–71; Stegmaier & Bartnick, *supra* note 20 at 675–76.

breach should have followed.[156] This practice, the critics charge, fails to provide companies with sufficient advance warning about what is required in order to provide acceptable data security.[157]

Companies like LabMD and Wyndham have 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."[158] 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."[159] An implication of this argument is that the FTC is engaging in a form of rulemaking through its cases, and making rules is beyond its powers in this area because the FTC lacks specialized rulemaking authority under Section 5.[160] 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.[161]

---

156 *See* Wyndham Amicus Brief, *supra* note 72, at 7–8.

157 *See id.*

158 Respondent LabMD, Inc.'s Motion to Dismiss Complaint with Prejudice & to Stay Admin. Proceedings, *supra* note 155, at 23–24.

159 Wyndham Reply in Support of Motion to Dismiss, *supra* note 18, at 7.

160 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?*, SELLERBEWARE BLOG (Apr. 26, 2010), http://www.consumeradvertisinglawblog.com/2010/04/is-congress-putting-the-ftc-on-steroids.html; *see also* Fed. Trade Comm'n, OPERATING MANUAL § 7.2.3.1, https://www.ftc.gov/sites/default/files/attachments/ftc-administrative-staff-manuals/ch07rulemaking.pdf ("Section 202(a) of Magnuson-Moss provides that the Commission's § 18 authority is its only authority to promulgate rules respecting unfair or deceptive acts or practices.").

161 *See, e.g.*, Nat'l Petrol. Refiners Ass'n v. FTC, 482 F.2d 672, 682–83 (D.C. Cir. 1973) (favoring formal rulemaking over policymaking via case-by-case adjudication because rulemak-

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.[162]

Instead, the FTC has opted to defer to industry to set the appropriate standards for good data security practices by utilizing a "reasonableness" standard.[163] In a statement issued in conjunction with the FTC's fiftieth data security settlement, the FTC stated,

> The touchstone of the Commission's approach to data security is reasonableness: a company's data security measures must be reasonable and appropriate in light of the sensitivity and volume of consumer information it holds, the size and complexity of its business, and the cost of available tools to improve security and reduce vulnerabilities.[164]

Almost all data security regulatory regimes that use a reasonableness standard include four critical aspects necessary for data security to be reasonable:

- Identification of assets and risk;
- Data minimization;
- Administrative, technical and physical safeguards; and
- Data breach response plans.[165]

These factors are reflected in the FTC's data protection jurisprudence as well as the FTC's Statement accompanying its fiftieth data security settlement.[166]

---

ing gives advance notice of required conduct and allows stakeholders to offer relevant perspectives on proposed regulation).

162 *See supra* note 52 and accompanying text; *see also* NAT'L INST. OF STANDARDS & TECH., FRAMEWORK FOR IMPROVING CRITICAL INFRASTRUCTURE CYBERSECURITY 2 (2014), http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214-final.pdf (explaining benefits of framework approach for organizations that will continue to face "unique risks").

163 *See* FED. TRADE COMM'N, COMMISSION STATEMENT MARKING THE FTC'S 50TH DATA SECURITY SETTLEMENT 1 (2014), http://www.ftc.gov/system/files/documents/cases/140131gmr-statement.pdf.

164 *Id.*

165 *See id.* (discussing "basic principles" of reasonable data-security practices).

166 *Id.* The Commission stated:

> These materials explain that, while there is no single solution, such a program follows certain basic principles. First, companies should know what consumer information they have and what employees or third parties have access to it. Understanding how information moves into, through, and out of a business is essential to assessing its security vulnerabilities. Second, companies should limit the

A reasonableness standard is already one of 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 [must] 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."[167] 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."[168] There are a number of other states that also require "reasonable" data security practices.[169] Regulations under FCRA require that certain employers

> information they collect and retain based on their legitimate business needs so that needless storage of data does not create unnecessary risks of unauthorized access to the data. Third, businesses should protect the information they maintain by assessing risks and implementing protections in certain key areas—physical security, electronic security, employee training, and oversight of service providers. Fourth, companies should properly dispose of information that they no longer need. Finally, companies should have a plan in place to respond to security incidents, should they occur.

Id.

167 MD. CODE ANN., COM. LAW § 14-3503(a) (LexisNexis 2013).

168 CAL. CIV. CODE § 1798.81.5 (West 2009).

169 *See* ARK. CODE ANN. § 4-110-104(b) (2011) ("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."); NEV. REV. STAT. ANN. § 603A.210(1) (LexisNexis 2010) ("A 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)–(b) (2013) (requiring "reasonable measures," including: "(1) 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)–(2) (West 2011) (providing that "[a]ny 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"); 11 R.I. GEN. LAWS ANN. § 11-49.2-2(2) (West 2006) ("A business that owns or licenses computerized unencripted personal information about a Rhode Island resident

"properly dispose" of customer information by taking "reasonable measures" to protect against the unauthorized access and possession of the information.[170] 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 are conducted and security policies and procedures are documented.[171]

Reasonableness standards permeate many traditional legal concepts. Many contractual obligations are also hitched to reasonableness[172] and the entire tort of negligence is largely a duty to act reasonably under the circumstances.[173] Indeed, this fact was explicitly acknowledged by FTC Commissioner Joshua Wright, writing for a unanimous Commission in denying LabMD's motion to dismiss:

> 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.[174]

As Commissioner Wright noted, tort liability can be as unpredictable as FTC enforcement, and torts can involve "compensatory and even punitive damages."[175] 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."[176]

---

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) (LexisNexis 2013) ("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; and (b) destroy, or arrange for the destruction of, records containing personal information that are not to be retained by the person.").

170 16 C.F.R. § 682.3(a) (2014).

171 45 C.F.R. §§ 164.306–.316 (2014).

172 *See, e.g.*, Kungys v. United States, 485 U.S. 759, 786 (1988) (Stevens, J., concurring in the judgment) (discussing reasonableness in the context of a claim of misrepresentation).

173 *See, e.g.*, Yarborough v. Alvarado, 541 U.S. 652, 674 (2004) (Breyer, J., dissenting) ("In negligence suits, for example, the question is what would a 'reasonable person' do 'under the same or similar circumstances.'").

174 Order Denying Respondent LabMD's Motion to Dismiss, *supra* note 19, at 17.

175 *Id.*

176 *Id.*

Reasonableness is also the locus for Fourth Amendment analysis of searches.[177] 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.[178]

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.[179] Indeed, any broad standard will follow this evolutionary trajectory.[180] Such a developmental pattern is inevitable if prior decisions have any kind of precedential effect or the functional equivalent of precedent.[181] The standard will start out rather broadly, but each new case will bring a new application of that standard to a concrete situation.[182] 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 United States, there is an overarching and very powerful norm for consistency across decisions and to avoid deviating from prior decisions.[183] 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

177 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' . . . .").

178 *See* Solove & Hartzog, *supra* note 7, at 619–20.

179 *See* Allan C. Hutchinson, *Work-in-Progress: Evolution and Common Law*, 11 TEX. WESLEYAN L. REV. 253, 254 (2005).

180 *See id.* at 254–57.

181 *See id.*

182 *See id.*

183 *See id.* at 254.

strict, adherence to those practices.[184] 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.[185] The FTC has not been engaging in rulemaking in disguise any more than when a court interpreting a statute over time is engaging in judicial legislation. This is just a common law system at work. This dynamic exists in many areas of the law. The norms and practices of the common law, such as adherence to precedent, apply to statutory and constitutional interpretation as well.[186]

The district 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."[187] 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.[188] Judge Salas seemed to understand that the rapidly evolving nature of data security made the FTC's analogies to the

184 *See* FED. TRADE COMM'N, *supra* note 163.

185 *See* FTC v. Wyndham Worldwide Corp., 10 F. Supp. 3d 602, 621 (D.N.J. 2014) ("Indeed, '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 the courts and litigants may properly resort for guidance*.' [Wyndham] Hotels and Resorts' argument that consent orders do not carry the force of law, therefore, misses the mark." (citation omitted)).

186 *See* Solove & Hartzog, *supra* note 7, at 620 ("Indeed, the meaning of many provisions of constitutional and statutory law cannot be understood simply by looking to their text—the body of judicial decisions offering a gloss on those provisions is an essential component that must be consulted.").

187 *Wyndham*, 10 F. Supp. 3d at 618 (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)).

188 *See id.* at 619.

NLRB and OSHA persuasive as models for bringing enforcement actions without issuing particularized prohibitions.[189]

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.'"[190] The court validated a reasonableness approach built upon industry standards and shaped by administrative actions.[191] The court quoted *General Electric Co. v. Gilbert*,[192] noting 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*."[193]

The district 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."[194] 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 bringing *all* unfairness actions without first proscribing particularized prohibitions—a result that is in direct contradiction with the flexibility necessarily inherent in Section 5 of the FTC Act."[195]

Our previous research demonstrates the validity of the court's conclusion that the FTC's interpretations of the FTC Act in administrative adjudications provide sufficient guidance.[196] For example, at the time we wrote this Article, there were over forty FTC complaints and consent decrees regarding data security and we reviewed all of them.[197] When reviewed in their totality, far from being vague and arbitrary, we were able to compile a list of specific security practices

189 *See id.* at 620 ("[G]iven the rapidly-evolving nature of data security, the Court is not persuaded by [Wyndham] Hotels and Resorts' attempt to undermine the FTC's analogies involving the National Labor Relations Act and OSHA on the grounds that precedent is lacking.").

190 *Id.*

191 *See id.*

192 Gen. Elec. Co. v. Gilbert, 429 U.S. 125 (1976).

193 *Wyndham*, 10 F. Supp. 3d at 621 (quoting *Gen. Elec.*, 429 U.S. at 141–42).

194 *Id.*

195 *Id.*

196 *See* Solove & Hartzog, *supra* note 7, at 619–25 (arguing that the FTC settlements are akin to common law and provide guidance to practitioners).

197 *See id.* at 628 n.211.

that the FTC has deemed as inadequate.[198] Moreover, most of these bad practices are ones that clearly run afoul of industry standards or other regulation.[199] Like the data security requirements of HIPAA and GLBA,[200] the FTC has given notice through settlements and adjudications that failure to have reasonable physical, technical, and administrative safeguards constitutes an unfair trade practice.

Some critics protest that only detailed rules could provide the kind of guidance industry needs to protect personal data,[201] 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 specific standards develops in the industry 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.[202] Rather than wait decades for such an exhaustive consensus to develop, the FTC's case-by-case approach has allowed it to engage in the functional equivalent of codifying those rules and standards that have achieved sufficient consensus.[203] 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

198 *See id.* at 651–55.

199 *See id.* at 656.

200 *See supra* text accompanying notes 118–28.

201 *See, e.g.*, Jan M. Rybnicek & Joshua D. Wright, *Defining Section 5 of the FTC Act: The Failure of the Common Law Method and the Case for Formal Agency Guidelines*, 21 Geo. Mason L. Rev. 1287, 1314–15 (2014) (arguing in favor of formal policy statement).

202 *See* Solove & Hartzog, *supra* note 7, at 657 ("With regard to privacy, what constitutes good practice is more in dispute, although there are certainly some practices about which consensus has developed."); Nat'l Inst. of Standards & Tech., Summary of the Privacy Engineering Workshop at he National Institute of Standards and Technology: April 9–10, 2014, at 1 (2014), http://www.nist.gov/cyberframework/upload/privacy-workshop-summary-052114.pdf ("In the security field, risk management models, along with technical standards and best practices, are key components of improving security. . . . To date, the privacy field has lagged behind in the development of analogous components.").

203 *See* Solove & Hartzog, *supra* note 7, at 662.

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 should not only 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.

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 take on this role more fully.

For the most part, the FTC has been quite conservative in its data protection enforcement, more of a norm-codifier than a norm-maker.[204] Thus far, the FTC has developed its jurisprudence in a measured and modest way.[205] It is time for the FTC to become less conservative in its approach. Rapid technological change continues to vex courts and lawmakers and 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.[206] 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 of Congress passing any privacy-related legislation anytime soon, as demonstrated by regularly unsuccessful legislative proposals.[207] The FTC is one of the best hopes for guiding U.S. privacy law to a more coherent and stable regulatory system.

---

204 *Id.* at 662, 676.

205 *See supra* Part I.B.3.

206 Solove & Hartzog, *supra* note 7, at 587.

207 *See* Tim Lisko, *112th Privacy Legislation*, PRIVACYWONK (Feb. 7, 2012), http://www.privacywonk.net/2011/08/112th-privacy-legislation.php (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/ (providing a review of privacy-related legislation in 2011); *EPIC Bill Track Tracking Privacy, Speech, and Cyber-Liberties Bills in the 111th Congress*, EPIC, https://epic.org/privacy/bill_track.html (last visited Nov. 21, 2015) (showing the status of proposed privacy-related legislation).

A. Linchpin 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 linchpin 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 levels. We contend that this role is critical to the system's legitimacy and ability to function.

In contrast to most other countries, the United States regulates privacy with a sectoral rather than omnibus approach.[208] 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.[209] In several instances, particular sectoral laws leave gaps where entire industries lack privacy regulation.[210] These industries can be regulated in certain dimensions by certain state laws or common law torts, but a large portion of their activities can remain unregulated.

As the Internet matured in the 1990s, the gaps in the sectoral approach were quite significant.[211] For example, the healthcare industry and much of the financial services industry lacked federal privacy regulation.[212] These gaps eventually closed, but significant ones still remain.[213] For example, there is no federal law that regulates much of online commerce.[214] Merchants such as Amazon.com lack any federal sectoral law to regulate the privacy of personal data they collect and use when selling the majority of their products and services.[215] Critics of the sectoral regime abound.[216]

---

208 Solove & Hartzog, *supra* note 7, at 587.

209 *Id.*

210 *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.").

211 *See* Solove & Hartzog, *supra* note 7, at 590–91 (discussing failed attempts to apply privacy torts and existing statutory law to Internet privacy issues in mid-to-late 1990s).

212 *Id.* at 587.

213 *Id.*

214 *Id.*

215 *Id.*

216 *See, e.g.*, 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."); Joel R. Reidenberg, *Privacy in the Information Economy: A Fortress or Frontier for Individual Rights?*, 44 FED. COMM. L.J. 195, 236 (1992) [hereinafter Reidenberg, *Privacy in the*

Concerned about consumer confidence, online companies voluntarily made promises about data protection in their privacy policies.[217] 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.[218]

The making of promises in privacy policies was essentially a self-regulatory system.[219] Companies could voluntarily decide whether to make a promise or not.[220] 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.[221] 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 of privacy policies.[222] The Privacy Rights Clearinghouse stated that, regarding the mandatory privacy notices under the GLBA, "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 [the GLBA]."[223] Janger and Schwartz noted:

Information Economy] ("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."); 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.").

217 *See* Solove & Hartzog, *supra* note 7, at 593–94. Voluntary privacy policies were also established in an effort to preempt regulation by the federal and state governments. *Id.* The idea was that establishing privacy policies, a form of self-regulation, would convince policymakers that additional regulation was unnecessary. *Id.*

218 *Id.* at 594.

219 *Id.* at 593–94.

220 *Id.*

221 *Id.* at 595–96.

222 *See* Edward J. Janger & Paul M. Schwartz, *The Gramm-Leach-Bliley Act, Information Privacy, and the Limits of Default Rules*, 86 MINN. L. REV. 1219, 1230 (2002).

223 Tena Friery & Beth Givens, *2001: The GLB Odyssey—We're Not There Yet: How Con-*

> [The Clearinghouse's] conclusion has been echoed by Federal Trade Commission Chairman Timothy Muris, who summarized the net result of [GLBA] 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.[224]

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.

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.[225] The FTC's broad range of coverage spanned countless industries, thus plastering over the large gaps and crevices left in between sectoral laws.[226] The FTC also brought a thin layer of coherence to the whole system, and this coherence has gradually thickened over the years.[227]

The FTC currently remains a key linchpin in the U.S. data protection regulatory regime.[228] Its policing of privacy policies has matured into a more robust set of substantive requirements.[229] Norms around best privacy and data security practices have developed.[230] The FTC has increasingly looked to these norms to add flesh to the very broad concepts of deception and unfairness.[231]

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.[232] Self-regulation still plays a big role, with industry serving as the primary generator of best practice norms.[233] Far from

---

sumers Rial Privacy Notices and Recommendations for Improving Them, PRIVACY RTS CLEARINGHOUSE (Dec. 4, 2001), http://www.privacyrights.org/ar/fp-glb-ftc.htm.

224 Janger & Schwartz, *supra* note 222, at 1220 (quoting Timothy J. Muris, Remarks at the Privacy 100 Conference (Oct. 4, 2001), http://www.ftc.gov/speeches/muris/privisp1002.htm).

225 Solove & Hartzog, *supra* note 7, at 585, 599, 667.

226 *Id.* at 587.

227 *Id.* at 649.

228 *Id.* at 600, 604–05.

229 *Id.* at 648–49.

230 *Id.* at 662.

231 *Id.*

232 *Id.* at 586.

233 *See id.* at 656 ("[I]t would be quite rare to 'find an FTC data security case where there was a serious argument that the security practice met industry norms.'"); *id.* at 661 (explaining

being externally imposed, the norms the FTC has enforced have been developed by industry as well as consumer expectations.[234] 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.[235] The FTC was an essential component of the Safe Harbor agreement, which, before its invalidation by the European Union Court of Justice, allowed personal data to flow between the United States and European Union ("EU").[236] The EU did not find U.S. 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.[237] The United States 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.[238] Once again, the FTC turned promises that would otherwise have been too soft into a more hardened form of protection.[239]

Although the Safe Harbor agreement was invalidated by the European Union Court of Justice for failing to provide adequate protection to European citizens, the FTC's data protection enforcement authority, remains a key component for the negotiation of agreements governing the international exchange of personal information. The FTC is the only governing body in the United States capable of pro-

---

how industry standards and consumer expectations form the basis for substantive FTC standards).

234 *Id.* at 661.

235 *See id.* at 603–04. The Safe Harbor agreement was invalidated by the European Union Court of Justice on grounds that it failed to provide adequate safeguards to European citizens. *See* Press Release, Court of Justice of the European Union, The Court of Justice Declares That the Commission's US Safe Harbour Decision Is Invalid (Oct. 6, 2015), http://curia.europa.eu/jcms/upload/docs/application/pdf/2015-10/cp150117en.pdf.

236 FUTURE OF PRIVACY FORUM, THE US-EU SAFE HARBOR: AN ANALYSIS OF THE FRAMEWORK'S EFFECTIVENESS IN PROTECTING PERSONAL PRIVACY 2 (2013), http://www.futureofprivacy.org/wp-content/uploads/FPF-Safe-Harbor-Report.pdf.

237 *See id.* at 1.

238 *See id.* at 2.

239 *See id.* (explaining that FTC can bring enforcement actions under Section 5 of the FTC Act "should the certifying company fail to live up to its Safe Harbor obligations"): *id.* at 15–21 (discussing FTC enforcement actions under the Safe Harbor agreement).

viding broad data protections to data subjects, a typical requirement for international data exchange.[240]

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 United States, which is increasingly at odds with most other countries in the world with its more fragmented sectoral approach to data protection.[241] 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 FTC enforcement. Although it is unlikely the United States will ever have a European-style comprehensive data protection statute, it 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 is 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 EU countries and countries modeled after the EU regime, there is a central data protection authority.[242] A data protection authority ("DPA") is a governmental entity that is focused on regulating privacy and that does so across most industries.[243] In contrast, the

---

240 *See* Paul M. Schwartz, *The EU-U.S. Privacy Collision: A Turn to Institutions and Procedures*, 126 HARV. L. REV. 1966 (2013).

241 Solove & Hartzog, *supra* note 7, at 587.

242 Zaidi, *supra* note 216, at 171–72.

243 *See* EUROPEAN COMM'N, SAFEGUARDING PRIVACY IN A CONNECTED WORLD: A EUROPEAN DATA PROTECTION FRAMEWORK FOR THE 21ST CENTURY 8–9 (2012) [hereinafter SAFEGUARDING PRIVACY], http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0009:FIN:EN:PDF; Francoise Gilbert, *European Data Protection 2.0: New Compliance Requirements*

United States lacks a DPA.[244] Instead, various statutes and various different agencies regulate different industries—the HHS regulates privacy in healthcare, the Department of Education ("DoE") regulates privacy in education, the Federal Communications Commission regulates privacy in telecommunications, and so on.[245]

In this 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 the regulatory gaps and the less need for states to protect their citizens. There seems to be practically little 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.[246] Yet, the sectoral approach is increasingly causing confusion and inefficiency and is at variance with most of the rest of the world.[247] 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.[248]

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:

---

in Sight—What the Proposed EU Data Protection Regulation Means for U.S. Companies, 28 SANTA CLARA COMPUTER & HIGH TECH. L.J. 815, 817 n.13 (2012).

244 *See* Zaidi, *supra* note 216, at 172.

245 *See* 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, 1207 (2003); Reidenberg, *Privacy in the Information Economy*, *supra* note 216, at 201.

246 Gellman, *supra* note 245, at 1206–07 (arguing that alternatives to legislation should be considered because Congress could, at best, agree to "broadly stated general principles").

247 Solove & Hartzog, *supra* note 7, at 587.

248 Gellman, *supra* note 245, at 1183.

> 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.[249]

However, Gellman hesitates to embrace the FTC as a data protection authority, stating:

> The FTC's endorsement of a diluted version of [Fair Information Practices] 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.[250]

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.[251] Moreover, specific and feasible rulemaking authority and increased jurisdiction would be key additional assets for the FTC to perform more effectively 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.[252] 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.[253] Or it might not be regulated at all.

Other types of personal data held by other types of companies could be protected in different ways. If the data were part of an education record at a school, it would be regulated by Family Educational

---

249 *Id.* at 1184.

250 *Id.* at 1205.

251 Solove & Hartzog, *supra* note 7, at 585–86.

252 42 U.S.C. § 17932(a)–(b) (2012).

253 *See* Solove & Hartzog, *supra* note 7, at 587.

Rights and Privacy Act ("FERPA").[254] If it were part of a financial record held by a financial institution, it would receive a different set of protections.[255] And so on.

Certain uses could trigger common law tort actions, although with little success.[256] There could be contract law claims in connection with some uses.[257] 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.[258] For many privacy violations, there may 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.[259] Assuming the company does not have a privacy policy for the app, no protections are even promised. Indeed, this is a common practice for apps. A 2011 study by the Future of Privacy Forum found that seventy-five percent of the most downloaded mobile apps do not have a privacy policy at all.[260]

---

254 Family Educational Rights and Privacy Act (FERPA), 20 U.S.C. § 1232g (2012); *see id.* § 1232g(a)(4)(A).

255 *See, e.g.*, 12 U.S.C. § 3402 (2012) (describing exceptions for when government authorities may access financial records held by financial institutions)

256 *See* Solove & Hartzog, *supra* note 7, at 590–91.

257 *See id.* at 595–97.

258 Stegmaier & Bartnick, *supra* note 20, at 673–74.

259 *See* Joy L. Pritts, *Altered States: State Health Privacy Laws and the Impact of the Federal Health Privacy Rule*, 2 YALE J. HEALTH POL'Y L. & ETHICS 327, 344 (2002) (describing HIPAA's limited coverage).

260 *FPF Finds Nearly Three-Quarters of Most Downloaded Mobile Apps Lack a Privacy Policy*, FUTURE PRIVACY F (May 12, 2011), http://www.futureofprivacy.org/2011/05/12/fpf-finds-nearly-three-quarters-of-most-downloaded-mobile-apps-lack-a-privacy-policy/. Varying conclusions have been reported by other organizations, including the FTC itself. *See* FED. TRADE COMM'N, MOBILE PRIVACY DISCLOSURES: BUILDING TRUST THROUGH TRANSPARENCY 23 n.96 (2013), http://www.ftc.gov/sites/default/files/documents/reports/mobile-privacy-disclosures-building-trust-through-transparency-federal-trade-commission-staff-report/130201mobileprivacyreport.pdf (citing June 2012 study by the Future of Privacy Forum finding "that only 28% of paid apps and 48% of free apps available in Apple's iTunes app store included a privacy policy or link to a privacy policy on the app promotion page"); FED. TRADE COMM'N, MOBILE APPS FOR KIDS: DISCLOSURES STILL NOT MAKING THE GRADE 7 (2012), http://www.ftc.gov/sites/default/files/documents/reports/mobile-apps-kids-disclosures-still-not-making-grade/121210mobilekidsappreport.pdf ("Of the 400 [children's] apps reviewed, only 20% (81) contained any privacy-related disclosure on the app's promotion page, on the developer website, or within the app."); Geoffrey A. Fowler, *Tech Giants Agree to Deal on Privacy Policies for Apps*, WALL ST. J., Feb. 23, 2012, at B4 ("[California Attorney General Kamala D.] Harris said some 22 of the 30 most-downloaded mobile apps don't have privacy policies."); 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, 45 "of 101 popular apps for iPhone and Android phones . . . didn't provide privacy policies on their websites or inside the apps"); Cameron Scott, *Mobile App Stores to Require, Disclose Privacy Policies*, PCWORLD (last visited

This is why the FTC is needed. Its broad jurisdiction would likely cover these mobile app companies. The FTC could set a baseline of protections for consumer health data, or for all companies handling personal 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, this company would now run afoul of the FTC's new requirement of baseline security practices. The FTC has asserted that failing to provide adequate data security, even in the absence of a promise to provide security, is an unfair practice.[261] Moreover, the FTC has prohibited certain kinds of data gathering even when not inconsistent with that specific company's privacy policy.[262] 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 if certain kinds of sensitive consumer information are disclosed to third parties, such as geolocation data. In *Goldenshores Technologies*,[263] the FTC alleged that a mobile flashlight application "represented, expressly or by implication, that respondents may periodically collect, 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."[264]

According to the FTC, "[t]hese facts would be material to users in their decision to install the application."[265] Thus, failure to specifi-

---

Oct. 21, 2015), 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.)").

261 *See* Solove & Hartzog, *supra* note 7, at 643 (noting that the FTC's privacy jurisprudence requires that consumers are provided with notice and choice about what data about them is collected and used, generally in the form of privacy policies, and that failing to provide adequate data security, even in the absence of a promise to provide security, is an unfair practice).

262 *Id.* at 641.

263 Goldenshores Techs., LLC, FTC File No. 132-3087, 2014 WL 1493611 (F.T.C. Mar. 31, 2014).

264 *Id.* at *3 (complaint).

265 *Id.*

cally provide notice of the collection of geolocation data was seen as deceptive by the FTC.[266] 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 is in and of itself deceptive?

Critics of more expansive FTC enforcement might raise concerns that increased enforcement 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.[267] Industry standards have evolved and matured, and there is a robust group of privacy professionals, academics, advocates, and others who can provide feedback.[268] Early on, a more restrained approach was compatible 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.[269] 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 to the modern privacy regulatory scheme is because it is has a considerably broad and diverse toolkit from which to fashion remedies, allowing the Commission to redress nontraditional 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.

---

266 *Id.* at *3–4.

267 *See* Gellman, *supra* note 245, at 1185.

268 *See* Andrew Clearwater & J. Trevor Hughes, *In the Beginning . . . An Early History of the Privacy Profession*, 74 OHIO ST. L.J. 897, 897–98 (2013).

269 *See id.* at 899 n.5 (noting that passage of FCRA created "a bar of folks representing companies that were the subject of [FCRA privacy] investigations"); *infra* text accompanying notes 357, 361.

a. Redress for Nontraditional Forms of Harm

Contract law and tort law have not often been successfully applied to many of the issues involving the collection, storage, use, and disclosure of personal data—when courts have applied contract and tort theories to these issues, they have struggled significantly in the application.[270] More broadly, the law has struggled to recognize privacy violations and data security breaches as harms.[271] The 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.[272]

In rejecting the appellant's contention that an increased risk of identity theft is itself a harm, the Third Circuit stated that the "[a]ppellants 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."[273] Although some courts have granted standing to plaintiffs merely alleging threat of future harm,[274] plaintiffs are generally unable to succeed in tort and

---

270 Solove & Hartzog, *supra* note 7, at 590–91, 596–97; *see In re* iPhone Application Litig., 844 F. Supp. 2d 1040, 1049 (N.D. Cal. 2012) (dismissing constitutional right to privacy, unjust enrichment, and negligence claims in suit alleging that Apple allowed third-party apps to use customers' personal information for commercial purposes); *In re* JetBlue Airways Corp. Privacy Litig., 379 F. Supp. 2d 299, 305, 330 (E.D.N.Y. 2005) (dismissing trespass to property, unjust enrichment, and breach of contract claims against JetBlue when it allegedly transferred passengers' data to third party); Dyer v. Nw. Airlines Corps., 334 F. Supp. 2d 1196, 1197, 1200 (D.N.D. 2004) (dismissing breach of contract claim against Northwest Airlines when it allegedly transferred passengers' data to third party); Dwyer v. Am. Express Co., 652 N.E.2d 1351, 1352–53 (Ill. App. Ct. 1995) (affirming dismissal of cardholders' invasion of privacy and fraud claims against American Express when it allegedly rented information on their spending habits to third parties).

271 Reilly v. Ceridian Corp., 664 F.3d 38, 42 (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.").

272 *Id.* at 43.

273 *Id.* at 44.

274 *See, e.g.*, Krottner v. Starbucks Corp., 628 F.3d 1139, 1142–43 (9th Cir. 2010); Pisciotta v. Old Nat'l Bancorp, 499 F.3d 629, 634 (7th Cir. 2007); Cousineau v. Microsoft Corp., 992 F. Supp. 2d. 1116, 1122 (W.D. Wash. 2012).

contract-based claims for harm resulting from a data breach without concrete evidence of financial harm like credit card fraud or identity theft.[275]

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 either an increased risk of future harm and the cost to mitigate such risk, or loss of privacy and deprivation of the value of personally identifiable information ("PII") as actionable harms that would provide the plaintiffs with standing to bring negligence, invasion of privacy, and bailment claims.[276] Regarding increased risk of future harm, the court held that "[i]n 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.'"[277] Regarding the cost to mitigate the risk of harm, the court held that "[s]uch 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.'"[278]

The court in *Galaria v. Nationwide Mutual Insurance Co.*[279] 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, identity fraud, medical fraud, or phishing."[280] The court was simply unwilling to recognize harm for standing purposes regardless of whether data "is ever actually misused or the plaintiff ever suffers adverse consequences from the exposure."[281] Finally, the court rejected the plaintiff's argument that "they suffered an

---

275 *See, e.g.*, Katz v. Pershing, LLC, 672 F.3d 64, 78–80 (1st Cir. 2012); Amburgy v. Express Scripts, Inc., 671 F. Supp. 2d 1046, 1052–53 (E.D. Mo. 2009); *see also* LaCourt v. Specific Media, Inc., No. SACV 10-1256-GW(JCGx), 2011 WL 1661532, at *3–4 (C.D. Cal. Apr. 28, 2011) (finding plaintiffs lacked standing in suit arising from websites' alleged use of cookies to track users' Internet usage without their consent).

276 Galaria v. Nationwide Mut. Ins. Co., 998 F. Supp. 2d 646, 651, 654, 657–58 (S.D. Ohio 2014).

277 *Id.* at 654.

278 *Id.* at 657 (quoting Clapper v. Amnesty Int'l USA, 133 S. Ct. 1138, 1151 (2013)).

279 Galaria v. Nationwide Mut. Ins. Co., 998 F. Supp. 2d 646 (S.D. Ohio 2014).

280 *Id.* at 658.

281 *Id.*

injury-in-fact in the form of deprivation of the value of their PII."[282] The court was skeptical of the argument that PII has any inherent monetary value and stated that "[r]egardless 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."[283] The court appeared to require evidence of the market's response to compromised data, noting that

> 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 Plaintiff allege that any third party sold his PII and that Named Plaintiff was deprived of his rightful profit.[284]

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 "[a]n 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."[285]

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 breach as harmful.[286] 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

---

282 *Id.* at 659.

283 *Id.* at 660.

284 *Id.*

285 UNFAIRNESS STATEMENT, *supra* note 85, at 1073 n.12; *see also* 15 U.S.C. § 45(n) (2012) (granting power to declare acts unlawful if the acts cause or are likely to cause substantial injury to consumers).

286 *See supra* note 271 and accompanying text.

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 reply in support of 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, 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."[287]

The FTC responded that there need only be a likelihood of injury through actual financial losses, and that other 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 reestablishing recurring payments after the credit cards have to be changed for hundreds of thousands of consumers.[288]

In a remarkable footnote in Judge Salas's district court opinion in *Wyndham* recognizing the dispute over whether nonmonetary injuries are cognizable under Section 5, the court seemed amenable to recog-

---

287 Wyndham Reply in Support of Motion to Dismiss, *supra* note 18, at 7–8 (quoting 15 U.S.C. § 45(n)).

288 Transcript of Oral Argument at 126:5–13, FTC v. Wyndham Worldwide Corp., 10 F. Supp. 3d 602 (D.N.J. 2014) (Civil 13-1887 ES), 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 claims. *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,' 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." (citation omitted)); *supra* text accompanying notes 271–84.

nizing nonmonetary harm, stating "the Court is not convinced that non-monetary harm is, as a matter of law, unsustainable under Section 5 of the FTC Act."[289]

The other related FTC case adjudicated in federal court relies upon similar logic. In *FTC v. Neovi*,[290] the Ninth Circuit supported a lower court's finding that

> [i]t 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.[291]

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.[292] 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 from or endorsed by a friend.[293] 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

---

289 *Wyndham*, 10 F. Supp. 3d at 623 n.15. The court did not reach the issue, however, because it concluded the FTC had alleged a substantial injury for the purposes of a motion to dismiss. *Id.*

290 FTC v. Neovi, Inc., 604 F.3d 1150 (9th Cir. 2010).

291 *Id.* at 1158 (quoting FTC v. Neovi, Inc., 2009 WL 56130, at *4 (S.D. Cal. Jan. 7, 2009).

292 *See* Toni Scott Reed, *Cybercrime: Losses, Claims, and Potential Insurance Coverage for the Technology Hazards of the Twenty-First Century*, 20 FIDELITY L.J. 55, 58, 60 (2014).

293 *See id.* at 58.

choice, the tenets of the FTC's Section 5 prohibitions on deceptive and unfair trade practices.[294]

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.[295] A considerable portion of the FTC's enforcement against false advertising is against those who would exploit the elderly.[296] In the realm of privacy, COPPA was created to protect minors because they are seen as less capable of making informed decisions regarding disclosing personal information online.[297]

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 traditional privacy harms, 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.[298]

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."[299] As defined by Section 5, "'unfair or deceptive acts or practices' include[ ] such acts or practices involving foreign commerce that . . . cause or are *likely to cause* reasonably foreseeable injury within the United States."[300] Many privacy and data security harms are not immediately experienced. When data is leaked or exposed it 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

294 *See supra* text accompanying notes 111–12 (identifying exploitation of consumers as common thread in unfairness and deception actions).

295 *See id.*

296 *See* Victor E. Schwartz & Cary Silverman, *Common-Sense Construction of Consumer Protection Acts*, 54 U. KAN. L. REV. 1, 9–11 (2005).

297 *See* Ryan Calo, *Digital Market Manipulation*, 82 GEO. WASH. L. REV. 995, 1034 (2014) (citing COPPA as an example of a special protection for children, a vulnerable population)

298 *See id.* at 1024–31 (arguing that "digital market manipulation" can harm consumers); Daniel J. Solove, *Introduction: Privacy Self-Management and the Consent Dilemma*, 126 HARV. L. REV. 1880, 1891–93 (2013).

299 UNFAIRNESS STATEMENT, *supra* note 85, at 1073 n.12.

300 15 U.S.C. § 45(a)(4)(A) (2012) (emphasis added).

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 dispersed societal impact rather than a concentrated 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 sting: "One bee sting can be shrugged off, but a hundred or a thousand can be lethal."[301] With each sting, the law typically turns its back and finds the harm not worth addressing. However, 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.

In contrast, 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.[302] Indeed, this seems to be one of the contemplated categories of "substantial injury" from an unfair practice.[303] 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.[304] According to the FTC, "[t]hese [societal costs] include not only the costs to the parties directly before the agency, but also the burdens on society in general in the form of increased paperwork, increased regulatory burdens on the flow of information, reduced incentives to innovation and capital formation, and similar matters."[305]

---

301 Solove, *supra* note 298, at 1891.

302 *See* UNFAIRNESS STATEMENT, *supra* note 85, at 1073 n.12; *supra* text accompanying note 285.

303 FTC v. Neovi, Inc., 604 F.3d 1150, 1157 (9th Cir. 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.'") (quoting Am. Fin. Servs. Ass'n v. FTC, 767 F.2d 957, 972 (D.C. Cir. 1985)).

304 UNFAIRNESS STATEMENT, *supra* note 85, at 1073–74.

305 *Id.*

The FTC is able to consider a more complete range of concerns than those addressed by contract and tort law, and is thus able to achieve a balance that is more subtle and more 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."[306] These two inquiries are not distinct, as the decision on whether a consumer injury is substantial informs the evaluation of unfairness.[307]

The FTC thus has a broader and more nimble conception of harm than 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 legal standards poorly designed to accommodate the nature of these harms.[308] 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 institutional bargaining has on consumer privacy. Increasingly, consumers' relationships with companies are negotiated through institutions, and those consumers are put at the mercy of the organizations negotiating their fate. For example, when K-12 schools, as well as colleges and universities, negotiate contracts with cloud-service providers or other data services, these contracts often fall short of protecting student privacy.[309]

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 often lacked essential

---

306 *Id.* at 1074.

307 *See, e.g.*, FTC v. Wyndham Worldwide Corp., 10 F. Supp. 3d 602, 622 (D.N.J. 2014) (noting that substantial injury is one element of unfairness claim); *Neovi*, 604 F.3d at 1155 (same).

308 *See, e.g.*, *In re* Sci. Applications Int'l Corp. (SAIC) Backup Tape Data Theft Litig., 45 F. Supp. 3d 14, 19, 31–32 (D.D.C. 2014) (struggling to find causation for standing in data breach case); *In re* Google, Inc. Privacy Policy Litig., 58 F. Supp. 3d 968, 980–89 (N.D. Cal. 2014) (dismissing class action for privacy violations for failure to state a claim); *In re* iPhone Application Litig., 844 F. Supp. 2d 1040, 1069 (N.D. Cal. 2012) (dismissing plaintiff's claim that storage of privacy-violating geolocation data constituted trespass).

309 *See* 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 (noting that school districts often fail to provide adequate notice to parents about use of cloud services and that none of the agreements with cloud vendors specifically prohibited marketing of students' information).

terms for the protection of student data.[310] Many of the analyzed agreements failed to give the school districts the right to audit and inspect the vendor's practices with respect to the transferred data.[311] The agreements also failed to prohibit or limit re-disclosure of student data or other confidential information.[312] No agreement "specifically prohibited the sale and marketing of children's information."[313]

Consumers are caught in the crossfire because their interests are often ignored in these contracts unless the schools fight for them. In the context of schools, the DoE under FERPA has very little ability to do much about this lack of representation, and, unlike HHS, the DoE has no direct authority to regulate companies receiving education records.[314]

Currently, the FTC is likely unable to regulate nonprofit schools as they are not engaged in commercial activity as long as they refrain from making a profit or providing other "benefit" to their members.[315] However, in similar situations involving for-profit companies, the FTC has alleged that a company's failure to adequately choose, contract

310 JOEL REIDENBERG ET AL., CTR. ON LAW & INFO. POLICY, PRIVACY AND CLOUD COMPUTING IN PUBLIC SCHOOLS 18–26 (2013), http://ir.lawnet.fordham.edu/clip/2. For example, the report notes that 95% of school districts use cloud services. *Id.* at 19. They are sharing sensitive student data with these third-party cloud-service providers. *Id.* at 5. Yet "approximately 20% of the responding districts had no policies addressing teacher use of information resources." *Id.* at 24.

311 *See id.* at 25.

312 *See id.* at 29–30.

313 *Id.* at 29.

314 *See* 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) ("[T]he language of the statute 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) (2000))); 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 clause legislation, [the Department of Education] enforces FERPA's provisions through the disbursement or rescission of federal education funds.").

315 *See* Cal. Dental Ass'n v. FTC, 526 U.S. 756, 766 (1999) (contemplating that "an organization devoted solely to professional education may lie outside the FTC Act's jurisdictional reach"); Cmty. Blood Bank of Kan. City Area, Inc. v. FTC, 405 F.2d 1011, 1019–20 (8th Cir. 1969) (finding a corporation does not fall under FTC jurisdiction "so long as its income is devoted exclusively to the purposes of the corporation, and not distributed to members or shareholders," because "it surely does not cease to be a nonprofit corporation merely because it has income, or keeps its books and records (as indeed the law might require it to) in much the same manner as commercial enterprises.").

with, and oversee a data service provider constituted an unfair and deceptive trade practice.[316] The case, *GMR Transcription Services, Inc.*,[317] involved the inadvertent exposure of people's medical data maintained by GMR, a company that provides medical transcription services.[318] 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."[319] Moreover, the FTC faulted GMR for failures in properly contracting with its data service provider.[320] 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 to typists (e.g., through encryption) and authenticating typists (e.g., through unique user credentials) before granting them access to such files; and . . . take adequate measures to monitor and assess whether Fedtrans employed measures to appropriately protect personal information under the circumstances.[321]

The FTC additionally found GMR to be deficient in doing due diligence before hiring its data service provider.[322] Looking broadly at the complaint, there are three key things that the FTC is now requiring companies to do when 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.[323]

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 noncommercial entities that engage in practices that result in consumer harm.

---

316 *See* GMR Transcription Servs., Inc., FTC File No. 122-3095, 2014 WL 4252393, at *4 (F.T.C. Aug. 14, 2014) (complaint).

317 GMR Transcription Servs., Inc., FTC File No. 122-3095, 2014 WL 4252393 (F.T.C. Aug. 14, 2014).

318 *Id.* at *2–3 (complaint).

319 *Id.* at *3.

320 *Id.*

321 *Id.*

322 *Id.*

323 *See id.* at *3–4.

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 *Vision I Properties*,[324] the FTC brought an action against a company that provided software to create customized shopping cart pages for other companies.[325] Vision I rented people's personal data, which it collected through its shopping cart software, to third-party direct marketers.[326] This practice was in violation of some of the privacy policies of the companies using Vision I's software.[327] 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.[328] 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 taken several steps to develop its theory of data security that requires companies holding personal information to ensure that third-party recipients will safeguard any data the company shares.[329] Specifically, the FTC has filed complaints of unfairness

---

324 Vision I Properties, LLC, FTC File No. 042-3068, 2005 WL 1274741 (F.T.C. Apr. 19, 2005).

325 *Id.* at *1.

326 *Id.* at *1–2.

327 *Id.* at *2.

328 *See id.* at *1–2.

329 *See* Daniel J. Solove & Woodrow Hartzog, *The FTC and Privacy and Security Duties for the Cloud*, 13 BNA PRIVACY & SECURITY L. REP. 577, 580 (2014). For examples of FTC critiques of inadequate third-party access control, see, e.g., Wyndham Complaint, *supra* note 2, at 12; Complaint at 7, United States v. Rental Research Servs., Inc., No. 09-cv-524 PJS/JJK (D. Minn. Mar. 5, 2009), http://www.securityprivacyandthelaw.com/uploads/file/FTC%20v_%20RRS%20Complaint.pdf; Complaint for Civil Penalties, Permanent Injunction, & Other Equitable Relief at 5, United States v. ValueClick, Inc., No. CV08-01711 MMM (RZx) (C.D. Cal. Mar. 13, 2008), https://www.ftc.gov/sites/default/files/documents/cases/2008/03/080317complaint.pdf; Upromise, Inc., FTC File No. 102-3116, 2012 WL 1225058, at *3–4 (F.T.C. Mar. 27, 2012) (complaint); ACRAnet, Inc., 152 F.T.C. 367, 368–69 (2011) (complaint); Premier Capital Lending Complaint, *supra* note 144, at 3–4; Nations Title Agency Complaint, *supra* note 144, at 2. This includes failure to verify and authenticate the identities of third-party recipients as well as failure to

against companies it alleged failed to verify and authenticate identity of third-party recipients,[330] failed to monitor data recipients' activity,[331] and failed to require by contract third-party protection of information.[332] Elsewhere, we have noted that there are two emerging strands of FTC jurisprudence that can address the consumer vulnerabilities inherent in institutional bargaining.[333] We noted, "[t]he first [strand] 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."[334] We argued 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 handlers, like] cloud provider[s]."[335] "Likewise," we argued that 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."[336]

The FTC should apply this theory to other privacy-based requirements, "such as requirements for confidentiality and data minimization and prohibitions on re-identification, data mining, and certain kinds of advertising and marketing to those identified" in the data.[337]

---

monitor or otherwise identify unauthorized recipient activity. *See* Complaint for Civil Penalties, Permanent Injunction, & Other Equitable Relief at 4–6, United States v. ChoicePoint Inc., No. 1 06-CV-0198 (N.D. Ga. Feb. 15, 2006) [hereinafter ChoicePoint Complaint], http://www.ftc.gov/os/caselist/choicepoint/0523069complaint.pdf (discussing defective verification policies). It also includes general charges of failing to protect information in the hands of 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 144, at 4.

330 *See, e.g.*, ChoicePoint Complaint, *supra* note 329, at 5 (admonishing company for accepting contradictory verification documentation).

331 *See* ChoicePoint Complaint, *supra* note 329, at 9.

332 *See* Nations Title Agency Complaint, *supra* note 144, at 4. 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) (setting out violations of Safeguards Rule); Nations Title Agency Complaint, *supra* note 144, at 3–4 (same).

333 Solove & Hartzog, *supra* note 329, at 578.

334 *Id.*

335 *Id.*

336 *Id.*

337 *Id.* at 580.

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 Part, 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."[338] 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 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.[339] Additionally, the previously mentioned requirements of materiality,[340] balancing,[341] and harm[342] facially limit the scope of valid complaints alleging unfair and deceptive trade practices.

Under the Administrative Procedure Act ("APA"),[343] the FTC is also prohibited from acting arbitrarily or capriciously, or abusing its discretion.[344] Although actions must be extreme to be labeled arbi-

338 Cass R. Sunstein, *Social Norms and Social Roles*, 96 Colum. L. Rev. 903, 909 (1996); *see infra* text accompanying note 364.

339 *See supra* note 16.

340 *See supra* note 89 and accompanying text.

341 *See supra* text accompanying notes 304–06.

342 *See supra* note 303 and accompanying text.

343 Administrative Procedure Act (APA), 5 U.S.C. §§ 551–559, 701–706 (2012).

344 5 U.S.C. § 706.

trary, capricious, or an abuse of authority,[345] this limit prohibits a blind disregard the FTC's delegated power.[346] Professor 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.[347]

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."[348]

---

345 *See* Comment, *Abuse of Discretion: Administrative Expertise vs. Judicial Surveillance*, 115 U. PA. L. REV. 40, 41–42 (1966) (noting that courts avoid striking down agency decisions unless the agency "has clearly acted unreasonably").

346 *See* Am. Horse Prot. Ass'n v. Lyng, 812 F.2d 1, 4–5 (D.C. Cir. 1987) ("Review under the 'arbitrary and capricious' tag line . . . encompasses a range of levels of deference to the agency, and . . . 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) (quoting State Farm Mut. Auto. Ins. Co. v. Dep't of Transp., 680 F.2d 206, 221 (D.C. Cir. 1982), *vacated on other grounds*, 463 U.S. 29 (1983))).

347 Jeff Sovern, *Private Actions Under the Deceptive Trade Practices Acts: Reconsidering the FTC Act as Rule Model*, 52 OHIO ST. L.J. 437, 442 (1991) (alteration in original) (footnotes omitted) (quoting 15 U.S.C. § 45(b) (1988)).

348 Atieh v. Riordan, 727 F.3d 73, 75–76 (1st Cir. 2013) (citation omitted) (first quoting 5 U.S.C. § 706(2)(A); then quoting Associated Fisheries of Me., Inc. v. Daley, 127 F.3d 104, 109 (1st Cir. 1997)); *see also* Managed Pharmacy Care v. Sebelius, 716 F.3d 1235, 1244 (9th Cir. 2013) (noting that the APA's review standard "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)); 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

As previously noted, the FTC must also provide fair notice to those it regulates.[349] Gerard M. Stegmaier and Wendell Bartnick note that "[t]he 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."[350]

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.[351] 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,[352] 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.[353] 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

---

of the law, on factual findings that are not supported by substantial evidence, or represents an unreasonable judgment in weighing relevant factors."); Henry v. INS, 74 F.3d 1, 4 (1st Cir. 1996) ("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."); Diaz-Resendez v. INS, 960 F.2d 493, 495 (5th Cir. 1992) (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").

349 *See supra* Part I.B.3.

350 Stegmaier & Bartnick, *supra* note 155, at 19.

351 *See, e.g.*, Scott, *supra* note 6, at 170.

352 *See supra* note 233 and accompanying text.

353 *See supra* Part I.B.3.

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 exhibited thus far. In the early days of FTC data protection enforcement, so many privacy norms had yet to develop. Most companies lacked privacy officers.[354] There was barely a privacy bar.[355] 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.[356] 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-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.[357]

These counselors have a nuanced understanding of the significance of the FTC complaints and are able to rely on the FTC's guidance as well as industry standards to competently advise their clients.[358] 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, but 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 the FTC's role depends partially on the extent of its influence on privacy professionals. The FTC has limited resources[359] and can only pursue a few privacy and data cases each

---

354 *See* Clearwater & Hughes, *supra* note 268, at 904 (estimating that first chief privacy officer in the United States was hired in mid-1990s).

355 *See id.* at 899 n.5.

356 *Id.* at 897–98.

357 *Id.* 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*, INT'L ASS'N PRIVACY PROFS: PRIVACY ADVISOR (Feb. 13, 2014), https://iapp.org/news/a/iapp-hits-15k-members/.

358 *See* Solove & Hartzog, *supra* note 7, at 585.

359 Sovern, *supra* note 347, at 442.

year.[360] One reason it is able to achieve broad enforcement 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 are updates in various other media forums.[361] In other words, whenever the FTC speaks, the privacy bar amplifies it and spreads the word. This helps to encourage companies to comply.

Once the FTC has brought an enforcement action based on a particular standard, that standard achieves a new level of legitimacy and formality. For all intents and purposes, the standard becomes law.[362]

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.[363] 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.

Given the amplifying and legitimizing role of FTC actions, the agency should be careful to avoid embracing norms that lack a fair degree of consensus. Sunstein has written that

> [e]xisting 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.[364]

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

---

360 Solove & Hartzog, *supra* note 7, at 600 (noting that the FTC brings roughly ten privacy-related cases per year).

361 *See, e.g.*, HUNTON & WILLIAMS: PRIVACY & INFO. SECURITY L. BLOG, https://www.huntonprivacyblog.com/ (last visited Oct. 21, 2015).

362 *See generally* Solove & Hartzog, *supra* note 7 (arguing that FTC rulings constitute a de facto common law of privacy).

363 *See id.*

364 Sunstein, *supra* note 338, at 909.

standards, the FTC has waited until norms and standards have developed and then begun enforcement."[365]

Though the FTC's direct and indirect powers are great, the FTC is still 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 oversteps, and that the FTC has budget and staff limitations and thus is "unlikely to expend its scarce resources on trivial deceptions."[366]

Moreover, there are certain types of harm that the FTC is not as well poised to redress. For example, compensatory remedies are better handled by tort law or other statutes because the FTC's role is largely to discourage bad behavior, not to compensate affected parties.[367] 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.[368] 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.

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 do 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.[369] 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

---

365 Solove & Hartzog, *supra* note 329, at 578.

366 Sovern, *supra* note 347, at 441–42.

367 *See* 15 U.S.C. § 45(a)(2) (2012) (empowering FTC to "*prevent* persons, partnerships, or corporations . . . from using unfair methods of competition" (emphasis added)).

368 Solove & Hartzog, *supra* note 7, at 600.

369 *See, e.g.*, GMR Transcription Servs., Inc., FTC File No. 122-3095, 2014 WL 4252393, at *1–4 (F.T.C. Aug. 14, 2014) (complaint) (alleging only that consumers were unaware of respondent's practices, but not explicitly identifying resulting harm).

not get the benefit of knowing when an FTC investigation did not result in the filing of a complaint.[370] The FTC does occasionally send closing letters to companies when they have investigated an alleged unfair or deceptive practice but have decided not to pursue an enforcement action.[371] However, 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. This information can be quite helpful to all companies in the industry, providing some indication as to which practices the FTC considered fair and truthful.

One good example of a closing letter regarding data security is the FTC's letter to Monster Worldwide, Inc. regarding a data security breach that resulted in the use of data of over a million customers who sought jobs using Monster's services in a targeted phishing campaign.[372] The FTC did not file a complaint against Monster.[373] According to the FTC:

> Our investigation of Monster sought to determine whether 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.[374]

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 risk; Monster's overall data security practices; the duration and scope of the compromise; the level of consumer injury; the type of infor-

370 *See* Allison Grande, *FTC Bureau Head Wants More Privacy Closing Letters Issued*, Law360 (Dec. 3, 2014, 9:59 PM), http://www.law360.com/articles/601348/ftc-bureau-head-wants-more-privacy-closing-letters-issued.

371 *See, e.g.*, Letter from Joel Winston, Assoc. Dir., FTC Div. of Privacy & Identity Prot., to Timothy C. Blank, Dechert, LLP (Mar. 6, 2008) [hereinafter Winston Closing Letter], http://www.ftc.gov/sites/default/files/documents/closing_letters/monster-worldwide-inc./monsterworldwide.pdf; *see also Staff Closing Letters*, Fed. Trade Comm'n, http://www.ftc.gov/enforcement/cases-proceedings/closing-letters-and-other-public-statements/staff-closing-letters (last visited Oct. 21, 2015).

372 Winston Closing Letter, *supra* note 371, at 1.

373 *See id.* at 1–2.

374 *Id.* at 1.

> mation disclosed without authorization; and Monster's overall response to the incident.[375]

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."[376]

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.[377]

The FTC then went 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 identity thieves and taking reasonable precautions to defend against such attacks.[378]

Thus, in this one letter in 2008, the FTC identified a threat to consumers and a corresponding obligation of companies, explained why the FTC did not pursue an enforcement action against the com-

---

375 *Id.* at 2.

376 *Id.*

377 *Id.*

378 *Id.*

pany under investigation, and provided explicit steps for fair data security practices to be followed by all parties handling consumer data.

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 article, the FTC is developing the functional equivalent of a common law of data protection.[379] 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 to how companies engage in data protection, and the FTC often focuses only 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 may do 99 out of 100 things right, make only one mistake, and be in violation of 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 to seek milder punishments and shorter auditing periods for companies that have done most things right and have made a good faith attempt at compliance. While the FTC does not enter into a twenty-year consent order with every company it files a privacy-related complaint against, this burdensome timescale is the most common duration for such agreements.[380] For some truly reckless organizations, this duration is likely justified. Yet for those companies that did many things right and other things wrong, a twenty-year consent order is overkill. The FTC should 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 Commission to increase the number of enforcement actions it brings.

---

379 Solove & Hartzog, *supra* note 7, at 606–25.

380 *Id.* at 606.

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 the new policy 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 immunity from prosecution. Furthermore, the new policy may incentivize the FTC to pursue a few more complaints in acknowledged industry gray areas 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.

If the FTC chooses to operate more in a gray zone, a proportionate punishment approach would allow the penalties to be lower than in those cases where there is already precedent addressing the particular issue. Companies should be expected to follow the FTC's jurisprudence in these gray areas much like they would follow any other common law standards in areas relevant to their business. When standards are clearly established, violations should be treated more harshly than when new standards are being recognized or developed.

If the FTC plans to take a bolder role on a new issue, recognizing a new standard or pushing the law forward in a more aggressive way, it should at first provide a little leeway to companies, taking a training wheels-style approach, with reduced punishment. After a reasonable time period, the training wheels should come off, and no leniency should be granted. If the FTC wants to develop the law at a greater pace, the process will likely go more smoothly under such a flexible, graduated penalty approach. This approach will also address concerns about fair notice raised by critics, which are likely to intensify if the FTC exercises its power more robustly.

There are other potential areas of improvement for the FTC. The FTC should make sure that its enforcement through consent orders that require compliance and ongoing assessment is effective.[381] As we noted earlier, the FTC would require assistance from Congress to ex-

---

381 *See* Chris Hoofnagle, *Assessing the Assessments*, FED. TRADE COMMISSION PRIVACY LAW & POL'Y (Sept. 28, 2015), https://hoofnagle.berkeley.edu/ftcprivacy/assessing-the-assessments/ (arguing "[t]he FTC is aware that it cannot effectively supervise all the companies under consent decree. Thus, in many cases, companies are required to perform an assessment but not required to submit it to the Agency. Doing so allows the FTC to avoid having knowledge of a problematic practice that is disclosed in an assessment, but not fully understood by the staff who review assessments.").

pand its jurisdiction to include noncommercial entities that are engaging in commercial practices.[382] Moreover, explicit rulemaking authority would be an essential tool for the FTC to develop more systematic rules where they are needed, 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 heavily on context. They cannot be readily reduced to a punch list, but instead involve a considerable amount of balancing of different values. Guidance and rules are 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 claiming that the FTC's data protection enforcement is exceeding its delegated 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 secure 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 initially conservative as it slowly began to regulate unfair and deceptive privacy-related practices. In the late 1990s, when the FTC first started bringing privacy-related complaints, it was unclear how privacy-related activities should be regulated and who should take the lead in doing so. However, 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 marketing manipulation, will continue to challenge policymakers.

---

382 *See supra* note 315 and accompanying text.

Now is the right time for the FTC to move boldly forward. The FTC has robust powers, and it should be make use of 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. Now, it is in the ideal position to take center stage and take U.S. data protection law to a new level.