RESPONSE

Due Process and the FTC's Fair and Reasonable Approach to Data Protection: Response to Woodrow Hartzog and Daniel J. Solove

*Vladimir J. Semendyai**

ABSTRACT

The Federal Trade Commission ("FTC") has long had authority to bring enforcement actions against "unfair or deceptive acts or practices in or affecting commerce" under section 5 of the Federal Trade Commission Act. In the last two decades, the FTC has used that authority to enforce data privacy and security in the digital age, constantly increasing its expertise in the area and the breadth of its enforcement. In their latest article, The Scope and Potential of FTC Data Protection*, Professors Hartzog and Solove argue that this is a good thing. They contend that the FTC should not only be allowed to continue its enforcement actions, but that it should expand its role as the linchpin of the American data security framework. Others, however, believe the FTC's approach to data protection enforcement raises some constitutional fair notice concerns.*

Until very recently, all companies targeted by the FTC for unfair data security practices had chosen to settle. This choice resulted in many consent orders and draft complaints, but few actual adjudication decisions. Professors

---

* J.D., 2016, The George Washington University Law School; B.S., Computer Science, 2005, University of Maryland. I owe many thanks to Daniel J. Solove for his thought-provoking lessons on Information Privacy Law and groundbreaking scholarship on the FTC regulation of data privacy and security that have made this Response possible. I am also grateful to Stephen Satterfield for his invaluable guidance throughout the development of this Response and to Dylan Scot Young, Julia Haigney, and the rest of the members and editors of *The George Washington Law Review* for their production and editorial work. Finally, I thank my wife, Blair, for her unwavering love and support.

Hartzog and Solove argue that these settlement documents are nonetheless the same as products of the traditional common law method and similarly provide adequate fair notice under the Due Process Clause.

This Response responds to their argument and contends that reliance on the FTC's settlement documents for fair notice is improper because the documents share very little substance with actual judicial decisions and are more analogous to contracts. Reliance on these documents, however, is not necessary because fair notice is already present in the FTC's enforcement approach, which relies on the reasonableness standard. This Response argues that under that approach, companies have constitutional fair notice because they only need to follow the data-security industry's best accepted practices for their circumstances in order to meet their duty of care. In addition, courts have long been familiar with applying the reasonableness standard in other contexts, most notably in tort law. Rather than tying fair notice to settlement documents that are inadequate for that role, looking to the reasonableness standard is the proper approach to the FTC's enforcement actions because it balances fair notice with the FTC's need to remain flexible in the ever-changing technological arena.

INTRODUCTION

Data breaches occur with growing frequency and are becoming a commonplace occurrence. There were nearly fifty percent more data breaches in 2014 than in 2013,[1] and 2015 saw more than 750 breaches causing the exposure of nearly 178 million personal information records, including those of children, from government agencies and private companies such as Ashley Madison, Experian, Anthem, and VTech.[2] Some have blamed this threat proliferation on companies using outdated data security strategies, likening this approach to "Einstein's definition of insanity: doing the same thing over and over again and expecting a different outcome."[3] In order to protect consumers and encourage companies to tighten their lax data security practices, the Federal Trade Commission ("FTC" or "Commission") has recently become more aggressive in its enforcement in the data privacy and security area.[4]

---

1 George V. Hulme, *Cybersecurity 2014: Breaches and Costs Rise, Confidence and Budgets Are Low*, CSO (Nov. 5, 2014, 11:54 AM), http://www.csoonline.com/article/2843820/data-protection/cybersecurity-2014-breaches-and-costs-rise-confidence-and-budgets-are-low.html [https://perma.cc/J74J-92PW].

2 James Eng, *Your Data at Risk: 2015 Was a Year Full of Memorable Hacks*, NBC NEWS (Dec. 23, 2015, 3:09 PM), http://www.nbcnews.com/storyline/2015-year-in-review/your-data-risk-2015-was-year-full-memorable-hacks-n474656 [https://perma.cc/3HLW-GZR7].

3 Tsion Gonen, *Data Breach Prevention Is Dead*, THE HILL (Feb. 09, 2015, 2:00 PM), http://thehill.com/blogs/congress-blog/technology/232041-data-breach-prevention-is-dead [https://perma.cc/A3C8-FMAP].

4 *See* Allison Grande, *FTC Steps Up Privacy Enforcement, with No Slowdown in Sight*, LAW360 (July 23, 2014, 7:36 PM), http://www.law360.com/articles/559907/ftc-steps-up-privacy-enforcement-with-no-slowdown-in-sight [https://perma.cc/NA4D-SZ4U].

In their new article, *The Scope and Potential of FTC Data Protection*, Professors Woodrow Hartzog and Daniel J. Solove argue that this change is a good thing.[5] Naming the FTC "the leading regulator of privacy"[6] in the United States and "the de facto U.S. data protection agency,"[7] they contend that not only are the Commission's efforts in the data protection context critical to the American approach to privacy regulation,[8] but that the FTC has been too reserved in those efforts and should further expand its data protection enforcement.[9] Because the Commission's statutory authority under section 5 of the Federal Trade Commission Act ("FTC Act")[10] is broad and flexible, they argue that it can uniquely adapt its enforcement strategies to meet the challenges posed by ever-evolving technologies.[11]

Yet not everyone agrees with what the FTC has been doing. Some critics have claimed that the FTC's case-by-case approach to data protection enforcement and its choice not to promulgate formal rules have left companies without constitutionally adequate fair notice of which data security practices violate section 5.[12] This criticism is featured prominently in the arguments made by Wyndham Worldwide Corporation, which challenged in a federal district court the FTC's authority to regulate data protection in the first place.[13]

---

5 Woodrow Hartzog & Daniel J. Solove, *The Scope and Potential of FTC Data Protection*, 83 GEO. WASH. L. REV. 101 (2015).

6 *Id.* at 138.

7 *Id.* at 105.

8 Professors Hartzog and Solove use the term "data protection" to collectively refer to both privacy and data security. *Id.* at 103. For consistency, this Response continues the practice.

9 *See id.* at 136–47.

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

11 Hartzog & Solove, *supra* note 5, at 116–17. Professors Hartzog and Solove have also previously published a comprehensive study of the history of the FTC, its rise to prominence within the data protection area, and the reasons behind that rise. *See* Daniel J. Solove & Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, 114 COLUM. L. REV. 583 (2014).

12 *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).

13 Motion to Dismiss by Defendant Wyndham Hotels & Resorts LLC at 8, 17, FTC v. Wyndham Worldwide Corp., 10 F. Supp. 3d 602 (D.N.J. 2014) (No. 13–1887(ES)); *see* Thomas O'Toole, *Wyndham Case Threatens to Put FTC Out of Data Security Business*, BLOOMBERG BNA (July 18, 2013), http://www.bna.com/wyndham-case-threatens-b17179875319/ [https://perma.cc/6KXU-LNN3]. A similar challenge on fair notice grounds was brought by LabMD, Inc. before the Commission. *See* Hartzog & Solove, *supra* note 5, at 114. Because the arguments made by LabMD closely mirror Wyndham's, this Response focuses only on the Wyndham case.

Wyndham's attack came in response to the complaint the Commission filed against it in federal court, alleging the hotel company's lax data security practices led to three separate breaches of its computer systems by hackers between 2008 and 2010, which caused the loss of 619,000 personal information records and over $10.6 million in fraudulent charges.[14] The FTC alleged that contrary to its promises to consumers, Wyndham "fail[ed] to implement reasonable and appropriate security measures"[15] by not using any firewalls or encryption at all and allowing continued use of default passwords on its systems.[16] Rather than acknowledge its responsibility, however, and settle with the Commission, Wyndham challenged the FTC's regulatory authority in the data protection context.[17] The hotel company argued that the FTC failed to provide it with constitutional fair notice because, based on the lack of any officially promulgated rules, it could not determine with "ascertainable certainty" what data protection practices it was required to adopt to avoid being unfair under section 5 and moved to dismiss.[18]

In 2014, the district court ruled against Wyndham[19] and the Third Circuit affirmed the decision on interlocutory appeal in 2015.[20] Both of those decisions are seminal in the development of data protection law because they mark the first time that federal courts explicitly endorsed the FTC's approach to regulating data protection under section 5 in the data breach context.[21] As discussed below, however, when it comes to the question of fair notice, some of the foundation underlying the reasoning behind both decisions is flawed and could have potentially negative impact on the development of data protection law, especially given the prominent role the decisions do and will continue to play in further discussions of the

---

14 First Amended Complaint for Injunctive & Other Equitable Relief at 12–18, FTC v. Wyndham Worldwide Corp., 10 F. Supp. 3d 602 (D.N.J. 2014) (No. 13–1887(ES)) [hereinafter Complaint]; Elinor Mills, *FTC Sues Wyndham Hotels over Data Breaches*, CNET (June 26, 2012, 9:46 AM), http://www.cnet.com/news/ftc-sues-wyndham-hotels-over-data-breaches/ [https://perma.cc/6DL9-ZDLU].

15 FTC v. Wyndham Worldwide Corp., 10 F. Supp. 3d 602, 609 (D.N.J. 2014) (quoting Complaint, *supra* note 14, at 17).

16 FTC v. Wyndham Worldwide Corp., 799 F.3d 236, 256 (3d Cir. 2015).

17 *See id.* at 240, 247.

18 *Id.* at 252–53, 255.

19 *Wyndham*, 10 F. Supp. 3d at 607.

20 *Wyndham*, 799 F.3d at 236, 259.

21 *See* GINA STEVENS, CONG. RESEARCH SERV., R43723, THE FEDERAL TRADE COMMISSION'S REGULATION OF DATA SECURITY UNDER ITS UNFAIR OR DECEPTIVE ACTS OR PRACTICES (UDAP) AUTHORITY 7–8 (2014), https://www.fas.org/sgp/crs/misc/R43723.pdf [https://perma.cc/D43P-HC9P] (discussing the history of the FTC's involvement with consumer privacy issues and data breaches under section 5 of the FTC Act).

FTC's role in that development.[22]

In rejecting Wyndham's fair notice argument, both the district court and the Third Circuit pointed to published consent orders and draft complaints from the Commission's previous unfairness actions as a source of sufficient fair notice.[23] A consent order is a settlement agreement between the Commission and the targeted company on security measures and auditing procedures the company must implement in the future.[24] It is usually accompanied by a draft of the Commission's complaint.[25] Settlement provides benefits to both sides—the FTC conserves scarce resources while companies can avoid the costs and the risks of protracted litigation and preserve their reputations by not being required to admit any wrongdoing.[26] These advantages have resulted in all but 3 of the over 170 FTC data protection actions ending in settlement.[27]

Professors Hartzog and Solove applaud the *Wyndham* courts' reliance on these settlement documents,[28] arguing that they give companies adequate notice of unfair data protection practices because they are the results of the FTC's "case-by-case adjudication over time" and follow "a developmental pattern typical of the common law."[29] In reality, however, by tying their fair notice analyses to these settlement documents, the *Wyndham* courts have built a weak foundation for their conclusions. Although both courts also analyzed unfairness in the data protection context under a reasonableness standard,[30] their subsequent reliance on what are essentially contracts and one-sided allegations shifted the focus from that standard, obscuring what is a much more adequate source of fair notice. This reliance further underscores the negative consequences of continued focus on documents that are not products of adjudication and that lack not only precedential value but also detailed reasoning behind the FTC's actions.

This Response argues that contrary to Professors Hartzog and Solove's contentions, the FTC's settlement documents do not provide

---

22 *See e.g.*, Hartzog & Solove, *supra* note 5, at 108–36.

23 *See Wyndham*, 799 F.3d at 257; *Wyndham*, 10 F. Supp. at 620–21. This Response refers to the consent orders and draft complaints collectively as "settlement documents."

24 *See generally* Solove & Hartzog, *supra* note 11, at 607, 610 (discussing consent orders).

25 *See* 16 C.F.R. § 2.31 (2014); ABA SECTION OF ANTITRUST LAW, CONSUMER PROTECTION LAW DEVELOPMENTS 239 (2009) [hereinafter CPLD].

26 *See* Solove & Hartzog, *supra* note 11, at 611–13.

27 *Id.* at 610–11.

28 *See* Hartzog & Solove, *supra* note 5, at 136.

29 *Id.* at 134; *see generally* Solove & Hartzog, *supra* note 11, at 619–27.

30 *See Wyndham*, 799 F.3d at 255–56; *Wyndham*, 10 F. Supp. 3d at 621.

constitutionally adequate fair notice of proper data protection practices. The FTC is still acting constitutionally, however, because another source of fair notice is available—a source that would be more evident if fair notice is decoupled from the FTC's settlement documents.

Part I of this Response analyzes the arguments in favor of finding adequate fair notice within the FTC's settlement documents and demonstrates that the specific characteristics of these documents make reliance on them for fair notice misplaced. Part II provides a better alternative for the source of fair notice, arguing that companies receive fair notice from accepted data protection practices established by the industry itself. This Part agrees with Professors Hartzog and Solove that, due to the constant improvements in computer technology and the self-regulatory nature of the data privacy regime in the United States, it would be impractical for the FTC to define with rigid exactness the protection practices it considers unfair. However, it argues that absent rigid rules, the solution is not to adopt the FTC's settlement documents as a substitute for those rules because they do not and cannot provide constitutional fair notice. Instead, the reasonableness of a given data protection strategy can be determined in advance by looking to the accepted practices of the industry itself and can be proven afterward in any legal action through data security expert testimony.

I. THE FTC'S SETTLEMENT DOCUMENTS FAIL AS SOURCES OF FAIR NOTICE

Professors Hartzog and Solove contend in their most recent article that the FTC's settlement documents provide clear guidance to companies and privacy professionals on the Commission's expectations in the data protection context.[31] These documents, however, fall far short of being able to provide any kind of constitutionally meaningful notice. Looking to them for that purpose only steers the discussion away from other sources for fair notice that better square the FTC's enforcement goals with constitutional requirements.

The main argument behind Professors Hartzog and Solove's fair notice analysis is the subject of their previous research—that these settlement documents are the new "common law" of privacy, having the full legal force that such a moniker implies.[32] Whatever the resolution of the heated debate over the appropriateness of such a label,[33] these settlement

---

31 *See* Hartzog & Solove, *supra* note 5, at 136.

32 *See id.* at 135; *see also* Solove & Hartzog, *supra* note 11, at 619–27.

33 Professors Hartzog and Solove have written extensively on the subject, endorsing

documents are significantly distinct from the body of impartial judicial decisions that serve as the foundation of traditional common law.[34] This distinction is critical to the question of whether any fair notice can be found within these documents and leads to the conclusion that it ultimately cannot. The lack of binding precedential force, the absence of reasoned and thoroughgoing analysis of the arguments on both sides of the dispute, and the fact that these settlement documents often are drafted to serve goals distinct from the development of a robust body of law are all key factors that not only distinguish these documents from the common law tradition,[35] but also make them wholly unsuitable as sources of constitutional fair notice.

One significant difference between the FTC's settlement documents and the judicial decisions that form the American common law tradition is that the former are not precedential.[36] The common law's adherence to precedent is one of its most fundamental characteristics and one that is particularly crucial to the fair notice argument.[37] Common law decisions provide future parties fair notice of what the law requires because they may rely on this precedent with the confidence that their cases will be adjudicated similarly.[38] This provides "a uniform starting point . . . from which future cases are evaluated, thereby ensuring a minimum measure of stability necessary to develop and maintain meaningful legal rules."[39]

---

the "common law" label that was first introduced by Christopher Wolf, a leading expert on privacy and data security in the digital age. *See, e.g.*, Testimony of Christopher Wolf, at 2, *In re* Digital Trade in the U.S. & Global Economies, USITC Inv. No. 332-540, (Feb. 28, 2013) http://www.hldataprotection.com/files/2013/03/USITC-Testimony-of-Christopher-Wolf2.pdf [https://perma.cc/5SK2-E6YG] ("The FTC effectively has created a 'common law' of what is expected from business when it comes to the collection, use, and protection of personal information."); Solove & Hartzog, *supra* note 11, at 619–27. Others, such as FTC Commissioner Wright, oppose this label because of the many differences between common law and the FTC's settlement documents, calling instead for the Commission to formally promulgate rules. *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, 1304–13 (2014).

34 Rybincek & Wright, *supra* note 33, at 1309–13.

35 *See id.*

36 *Id.* at 1305.

37 *See id.* at 1301; *see also* Morris L. Cohen, *The Common Law in the American Legal System: The Challenge of Conceptual Research*, 81 L. LIBR. J. 13, 15 (1989) ("*Common Law* . . . receives its binding force from immemorial usage and universal reception . . . . [and is t]hat body of rules, principles and customs . . . by which courts have been governed in their judicial decisions." (quoting NOAH WEBSTER, AMERICAN DICTIONARY OF THE ENGLISH LANGUAGE (1st ed. 1828)).

38 Rybnicek & Wright, *supra* note 33, at 1295–96, 1312.

39 *Id.* at 1312.

When circumstances change and a departure from precedent is necessary to reflect a shift in thinking or to deal with exposed shortcomings, any such departure is supported by a thorough examination of the issues as well as a reasoned explanation for the necessity of breaking tradition.[40] Parties are always on notice, therefore, about the scope of the relevant law and how the courts will handle their specific set of facts.

In contrast, the FTC's settlement documents have no such binding power. The FTC is not required to follow its own precedent and can change what it considers an unfair practice in the data protection area at any time and for any reason.[41] Even a change in the FTC's membership, which occurs often because Commissioners are appointed on a staggered basis every seven years,[42] and which inevitably generates changing viewpoints and political goals, may lead to a drastic alteration in how the FTC interprets unfairness in the data protection area. For example, Commissioner Wright recently described how his arrival and the departure of two other Commissioners led to a complete reversal in the FTC's stance on unfairness in another area of law.[43] This lack of precedential force makes these settlement documents unreliable as a source of fair notice because companies cannot use them to predict with any degree of certainty how the FTC will act in the future.

Professors Hartzog and Solove acknowledge this shortcoming in their recent article.[44] In response, they argue that the settlement documents have "the functional equivalent of precedent" because the Commission has remained consistent in its data protection enforcement.[45] However, there is no assurance that it will continue to remain consistent. The Commission can change course at any time, leaving companies at the mercy of its whims when it comes to fair notice of its expectations.

In addition to lacking all precedential value, the FTC's settlement documents also do not provide sufficient guidance because they are necessarily one-sided—they have not undergone the test of an adversarial adjudicative proceeding that has fully fleshed out both sides of the

---

40 *See id.* at 1299–1301.

41 *See* Beatrice Foods Co. v. FTC, 540 F.2d 303, 312 (7th Cir. 1976) ("[A] consent decree [is not] a controlling precedent for later Commission action."); Solove & Hartzog, *supra* note 11, at 607 ("[C]onsent orders legally function as contracts rather than as binding precedent.").

42 Solove & Hartzog, *supra* note 11, at 608.

43 Rybnicek & Wright, *supra* note 33, at 1313.

44 Hartzog & Solove, *supra* note 5, at 163 ("[P]resumably 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 [data protection] context . . . .").

45 *Id.* at 133–34; Solove & Hartzog, *supra* note 11, at 619–20.

dispute.[46] In fact, they typically lack any independent analysis of the targeted party's side because, unlike judicial decisions, which are issued after each side has had a chance to thoroughly explain and defend its arguments, the FTC's settlement documents are not the product of litigation, but of negotiation.[47] They present only the FTC's side and interpretation of the facts, omitting discussion of any arguments or defenses the targeted party may have relied on at trial.[48] As a result, companies find in these orders at best only half of the guidance needed to determine what data protection practices are reasonable.[49]

The characteristics above apply equally to both consent orders and draft complaints. Looking at each separately, however, does not change the outcome in considering their effect on the fair notice question. Consent orders appear to be the closer of the two to judicial opinions because they are prepared with both parties' input and issued at the conclusion of the FTC's proceedings. Nonetheless, the two are very distinct. Crucially, consent orders do not contain a thorough discussion of the underlying principles and reasoning behind the FTC's arguments,[50] a key component of judicial opinions and one critical to the fair notice analysis. Looking closely at the reasons for this omission glaringly exposes why consent orders are wholly inadequate as sources of fair notice, or, as the Third Circuit politely put it, "of little use to [companies] in trying to understand the specific requirements imposed by [section 5 of the FTC Act]."[51] Other courts have also treated consent orders as unreliable and unpersuasive in the litigation context.[52]

The lack of detailed reasoning in consent orders stems from the underlying goals of both parties to the settlement. A targeted company

---

[46] *See* Rybnicek & Wright, *supra* note 33, at 1308 ("[W]here a defendant is less interested in the precedential value of a case, the use of the common law approach may not result in the creation of efficient legal rules because the law will only ever change in a direction that favors the plaintiff.").

[47] *See* United States v. Armour & Co., 402 U.S. 673, 681 (1971) ("Consent decrees are entered into by parties to a case after careful negotiation has produced agreement on their precise terms.").

[48] *See* Rybnicek & Wright, *supra* note 33, at 1310.

[49] *Id.* at 1311.

[50] *Id.* at 1310–11.

[51] FTC v. Wyndham Worldwide Corp., 799 F.3d 236, 257 n.22 (3d Cir. 2015).

[52] *See, e.g.*, United States v. E.I. du Pont de Nemours & Co., 366 U.S. 316, 330 n.12 (1961) ("[T]he circumstances surrounding such negotiated [consent] agreements are so different that they cannot be persuasively cited in a litigation context."); Beatrice Foods Co. v. FTC, 540 F.2d 303, 312 (7th Cir. 1976) (dismissing as unpersuasive Beatrice's reliance on the FTC's prior consent orders because consent orders are "not [decisions] on the merits and therefore do[] not adjudicate the legality of any action by a party thereto").

desires that these orders be vague and general in their descriptions of unfairness because the company is negotiating to protect its business secrets and public image and is not concerned with providing notice or advancing the state of the law.[53] It is not even required to admit any fault.[54] The FTC, on the other hand, seeks only to ensure the targeted company's continued compliance with the settlement, thus further promoting the legitimacy of its enforcement activities.[55] The Commission chooses its targets carefully, focusing only on cases where it has a high chance of success and quick settlement while ignoring more complex cases where there is no obvious outcome.[56] The combination of these goals has resulted in consent orders that are vague and focus solely on unfair conduct, often not providing any explanation of what conduct the FTC considers fair,[57] or why the FTC found the same practices fair in one case and unfair in another.[58]

The FTC's draft complaints fare no better than the consent orders they accompany. Although the Commission will generally negotiate during settlement, as a matter of policy it does not negotiate the content of the complaint,[59] making it completely one-sided. Furthermore, these complaints also lack any rigorous reasoning in support of the FTC's

---

53 *See* Rybnicek & Wright, *supra* note 33, at 1310; *see also* Solove & Hartzog, *supra* note 11, at 611–13 (discussing the financial motivations for settling with the FTC).

54 Solove & Hartzog, *supra* note 11, at 610; *see also, e.g.*, Agreement Containing Consent Order at ¶ 5, EPN, Inc., also d//b/a Checknet, Inc., No. 112-3143 (F.T.C. June 7, 2012), https://www.ftc.gov/sites/default/files/documents/cases/2012/06/120607epnagree.pdf [https://perma.cc/G4Y6-FY67] ("This agreement is for settlement purposes only and does not constitute an admission by proposed respondent that the law has been violated as alleged in the draft complaint, or that the facts as alleged in the draft complaint, other than the jurisdictional facts, are true.").

55 *See* Douglas H. Ginsburg & Joshua D. Wright, *Antitrust Settlements: The Culture of Consent*, *in* 1 WILLIAM E. KOVACIC: AN ANTITRUST TRIBUTE, *LIBER AMICORUM* 177, 181 (Nicolas Charbit et al. eds., 2012). Although this article is about the FTC's role in antitrust enforcement, similar analysis is applicable to consent orders in the data protection context.

56 *See* Solove & Hartzog, *supra* note 11, at 613 ("David Vladeck, a law professor and former director of the Bureau of Consumer Protection of the FTC, using data security complaints as an example, stated, '[FTC] [s]taff wouldn't bring a close case to the Commission. . . .'"); *see also* Jeff Sovern, *Private Actions Under the Deceptive Trade Practices Acts: Reconsidering the FTC Act as Rule Model*, 52 OHIO ST. L.J. 437, 444 (1991) (noting that in the deception context, "the FTC has generally used its power to produce rules which make it easy for the FTC to find [violations]").

57 *See* Hartzog & Solove, *supra* note 5, at 166–67 (noting that companies usually do not know when the Commission determines their practices were not unfair).

58 *See* Gerard M. Stegmaier & Wendell Bartnick, *Psychics, Russian Roulette, and Data Security: The FTC's Hidden Data-Security Requirements*, 20 GEO. MASON L. REV. 673, 700 (2013).

59 CPLD, *supra* note 25, at 239.

allegations because of the very nature of complaints—even under the modern heightened pleading standard, a complaint must only provide enough facts to make a claim plausible.[60] Plausibility, however, is a much lower standard of proof than the one the Commission would have to meet at trial,[61] requiring a less rigorous justification. Along with the deference that courts show the Commission in its interpretation of law and facts,[62] this lower standard of proof explains the dearth of detailed reasoning in the FTC's draft complaints.

Professors Hartzog and Solove nonetheless contend that the FTC's settlement documents are sufficient for fair notice because they are a product of "case-by-case adjudication over time" and form the FTC's "data protection jurisprudence."[63] They argue that the FTC follows the same "developmental pattern" with its settlement documents as courts do with traditional common law, supporting the conclusion that the Commission is engaging "in administrative adjudications [that] provide sufficient guidance."[64] But the FTC does not adjudicate—it negotiates and settles.[65] Many of the hallmarks of an adjudicatory proceeding, such as discovery, examination of witnesses, and a final decision made by a neutral decisionmaker, are missing from the settlement negotiation process.

Given these shortcomings of the FTC's settlement documents, it is striking that both of the *Wyndham* courts looked to them as a source of fair notice. In particular, the district court's explanation for finding fair notice is based on an analysis that is questionable at best.[66] To support its conclusion, the district court relied on a pair of Supreme Court decisions, *SEC v. Chenery Corporation*[67] and *General Electric Co. v. Gilbert*.[68] The court relied on *Chenery* to support its finding that the FTC may establish

---

60 *See* Bell Atl. Corp. v. Twombly, 550 U.S. 544, 570 (2007).

61 *Id.* at 556 ("Asking for plausible grounds to infer an agreement does not impose a probability requirement at the pleading stage . . . .").

62 *See* Sovern, *supra* note 56, at 444 (noting that, due to the deference accorded the FTC's interpretation of the law under section 5's deception prong, "the FTC may establish [a violation] on a much lesser showing than is required of a consumer suing a merchant in, say, a common law fraud or breach of warranty action").

63 Hartzog & Solove, *supra* note 5, at 134–35, 141.

64 *Id.* at 133–36.

65 *See* CPLD, *supra* note 25, at 239.

66 It would be remiss not to point out that the ability to analyze both of the *Wyndham* courts' opinions and their underlying reasoning is further evidence of the important role that fully reasoned and thoroughly explained judicial decisions play in providing guidance to future litigants and in the continued development of the law.

67 SEC v. Chenery Corp., 332 U.S. 194 (1947).

68 Gen. Elec. Co. v. Gilbert, 429 U.S. 125 (1976) (superseded by statute on other grounds).

rules not only through rulemaking, but also through adjudication in the form of orders.[69] The court then quoted the Supreme Court in *Gilbert*, which stated 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 the courts and litigants may properly resort for guidance*."[70] Professors Hartzog and Solove also quote this language to support their fair notice argument.[71]

Reading what the Supreme Court said in context, however, indicates that these cases support quite the opposite conclusion. *Chenery* specifically focused on the presence of a "thorough reexamination of the problem in light of the purposes and standards" of the statute—a reexamination that was "expressed . . . with *a clarity and thoroughness that admit[s] of no doubt as to the underlying basis of its order*."[72] Similarly, *Gilbert* goes on to state that "[t]he weight of such a[n administrative] judgment in a particular case will depend upon the *thoroughness evident in its consideration, the validity of its reasoning, [and] its consistency with earlier and later pronouncements* . . . ."[73] These assertions demonstrates that an agency's statements only have value when they contain developed and detailed reasoning behind its conclusions, the very characteristics that are fundamental to traditional common law and absent from the FTC's settlement documents.[74]

The Third Circuit's analysis of the usefulness of these settlement documents for fair notice is similarly weak. Although the court seemed to stop short of accepting them as products of adjudications[75] and limited its reliance only to the FTC's draft complaints,[76] it still gave the settlement documents more weight than they deserve. For example, the Third Circuit relied on *United States v. Lachman*,[77] noting that "courts regularly consider materials that are neither regulations nor 'adjudications on the merits.'"[78]

---

69 FTC v. Wyndham Worldwide Corp., 10 F. Supp. 3d 602, 617 (D.N.J. 2014) (citing *Chenery*, 332 U.S. at 202–03).

70 *Id.* at 621 (quoting *Gilbert*, 429 U.S. at 141–42).

71 Hartzog & Solove, *supra* note 5, at 135.

72 *Chenery*, 332 U.S. at 199 (emphasis added).

73 *Gilbert*, 429 U.S. at 142 (emphasis added) (quoting Skidmore v. Swift & Co., 323 U.S. 134, 140 (1944)).

74 *See supra* notes 50–62 and accompanying text.

75 *See* FTC v. Wyndham Worldwide Corp., 799 F.3d 236, 253–54, 257 (3d Cir. 2015) (accepting Wyndham's position that the FTC's settlement documents are not adjudications).

76 *See id.* at 257–58, 257 n.22.

77 United States v. Lachman, 387 F.3d 42 (1st Cir. 2004).

78 *Wyndham*, 799 F.3d at 257 (citing *Lachman*, 387 F.3d at 57).

Lachman, however, is hardly on point—it involved a void-for-vagueness challenge to a regulation and dealt with the question of whether informal statements by agency employees could be considered contradictory interpretations of that regulation.[79] The FTC, on the other hand, has not issued any data protection regulations at all, so any analysis under *Lachman* is misplaced.

Moreover, the Third Circuit's reliance on the Commission's settlement documents was at best dicta. The court stated clearly that the question it was deciding was "not whether Wyndham had fair notice of the *FTC's interpretation* of the statute, but whether Wyndham had fair notice of what the *statute itself* requires."[80] References to consent orders or draft complaints, however, appear only after the court resolved that question in a later discussion of what the FTC commissioners view as unfair data protection practices[81]—that is, exactly what the court earlier found irrelevant to the question it was deciding. Although only dicta, it is still a good example of the distorting effect that the mere branding of these settlement documents as "common law" is having on the discussion of fair notice within the context of data protection.

II. THE REASONABLE APPROACH TO FAIR NOTICE

If the FTC's settlement documents fail to deliver sufficient fair notice to satisfy constitutional requirements, must the FTC then stop enforcing data privacy in the United States, causing the privacy framework in this country to "lose nearly all its legitimacy?"[82] Of course not. Companies need not look beyond the Commission's reasonableness approach to data protection enforcement to receive fair notice of what practices they should adopt. The reasonableness standard is ideal for two reasons—it allows the FTC to continue to adapt quickly to the rapidly changing landscape of data protection technology, and it allows companies to defend easily against any unfairness action because courts have long understood that standard to satisfy the fair notice requirements of the Due Process Clause.

As Professors Hartzog and Solove point out, the FTC does not need to promulgate any formal guidelines because it can point to the best data protection practices developed by the industry itself.[83] This Response agrees that the Commission cannot and should not provide a "'check list'

---

79 *See Lachman*, 387 F.3d at 56–59.

80 *Wyndham*, 799 F.3d at 253–54.

81 *See id.* at 257.

82 Solove & Hartzog, *supra* note 11, at 604.

83 *See* Hartzog & Solove, *supra* note 5, at 129–31.

of data security practices . . . [applicable] in all contexts" because data protection technologies evolve too quickly for "a one-size-fits-all checklist" to be useful.[84] Instead, by applying the reasonableness approach, the FTC can maintain its flexibility—establishing through expert testimony that a company acted unreasonably by not implementing such data protection practices as are commonly considered appropriate.

The reasonableness standard has a long tradition in English and American common law,[85] and courts have long held that it satisfies constitutional fair notice requirements, most importantly in regulatory[86] and data protection[87] contexts. As Professors Hartzog and Solove detail, many state and federal data protection laws are already based on the reasonableness standard.[88] Furthermore, this approach has proven to be very effective in other areas of law where it would be impractical to define inappropriate behavior with exactness.[89] For example, courts have long applied the reasonableness standard and relied on expert testimony in medical malpractice actions.[90] The medical profession is governed by standards set by professional standards-setting bodies, and medical professionals must be licensed and are encouraged to complete strict certification processes before being able to practice medicine.[91] In medical

---

84 *Id.* at 130.

85 *See* Vaughan v. Menlove, (1837) 132 Eng. Rep. 490, 493 (establishing that the proper standard in a negligence action was to ask whether the defendant showed "a regard to caution such as a man of ordinary prudence would observe"); *see also* Brown v. Kendall, 60 Mass. (6 Cush.) 292, 298 (1850) (establishing that the correct test for a negligence claim is whether the defendant acted with a "degree of care and diligence . . . which men of ordinary care and prudence would use under like circumstances").

86 *See* Voegele Co., Inc. v. Occupational Safety & Health Review Comm'n, 625 F.2d 1075, 1078–79 (3d Cir. 1980) (applying a reasonable person test to regulations under the Occupational Safety and Health Act); *see also* Loschiavo v. City of Dearborn, 33 F.3d 548, 552–53 (6th Cir. 1994) ("A regulation is not rendered impermissibly vague simply because it calls for a judicial determination of 'reasonableness.'"), *abrogated on other grounds by* Johnson v. City of Detroit, 446 F.3d 614 (6th Cir. 2006). State courts have also long found statutes prohibiting negligent acts to be constitutional. *See, e.g.*, State v. Johnson, 653 P.2d 428, 432–33, 478 (Haw. 1982) (holding that a statute prohibiting negligent driving provided "fair notice sufficient to satisfy due process requirements").

87 *See In re* Zappos.com, Inc., No. 3:12-CV-00325-RCJ-VPC, 2013 WL 4830497, at *4–5 (D. Nev. Sept. 9, 2013) (stating that the defendant owed a "duty of care to act as a reasonable and prudent person under the same or similar circumstances" in safeguarding plaintiff's personal data).

88 *See* Hartzog & Solove, *supra* note 5, at 131–32 & nn.167–71.

89 *See id.* at 132–33.

90 Joseph H. King, *The Common Knowledge Exception to the Expert Testimony Requirement for Establishing the Standard of Care in Medical Malpractice*, 59 ALA. L. REV. 51, 51 (2007).

91 *See Board Certification and Maintenance of Certification,* AM. BD. MED.

malpractice actions, expert testimony is therefore necessary to establish a duty of care under those standards and to show how a given defendant violated that duty of care by acting unreasonably.[92] This permits the law to remain flexible enough to adapt to rapidly changing medical technologies and practices[93] while accounting for variables such as differences in geographic location and available resources.[94]

For the same reasons, the reasonableness approach is preferable in the data protection context. Much like the medical profession, data security practices rapidly change with new technological developments.[95] A company's available resources and the amount of personal data it maintains are also variant factors that must be considered in any unfairness determination.[96] The application of the reasonableness standard easily achieves this balance, particularly because the data security profession has become sufficiently established in recent years.[97] Companies can now turn to qualified experts certified by established certification organizations similar to medical certification boards.[98] These experts can explain the

---

SPECIALTIES, http://www.abms.org/board-certification/ [https://perma.cc/ZC84-CYZS] (last visited May 18, 2016).

92 King, *supra* note 90, at 51.

93 *See* Arti Kaur Rai, *Rationing Through Choice: A New Approach to Cost-Effectiveness Analysis in Health Care*, 72 IND. L.J. 1015, 1015 (1997) (describing the economic challenges of the rapid developments in medical technology); *see also Accelerating Change in Medical Education*, *Overview*, AMA, http://www.ama-assn.org/sub/accelerating-change/overview.shtml [https://perma.cc/E57Z-HU3X] (last visited May 18, 2016) (describing the AMA's goals to better adapt modern medical education to the "rapidly changing health care environment").

94 *See, e.g.*, Sommer v. Davis, 317 F.3d 686, 693 (6th Cir. 2003) (holding that an expert witness was properly excluded because he did not have knowledge of the standard of care in the location where the injury occurred); Primus v. Galgano, 329 F.3d 236, 241 (1st Cir. 2003) (stating that in Massachusetts, "it is permissible to consider the medical resources available to the physician [when] determining the skill and care required" (quoting Brune v. Belinkoff, 235 N.E.2d 793,798 (Mass. 1968))).

95 Wyndham's own privacy policy provides a good example. Between 2008 and 2010, Wyndham promised to protect its customers' data with such "industry standard practices" as 128-bit encryption. Complaint, *supra* note 14, at 9. Just a few short years later, however, cryptography experts were already questioning the efficacy of this level of encryption. *See* Bruce Schneier, *What Exactly Are the NSA's 'Groundbreaking Cryptanalytic Capabilities'?*, WIRED (Sept. 4, 2013 9:29 AM), http://www.wired.com /2013/09/black-budget-what-exactly-are-the-nsas-cryptanalytic-capabilities/ [https://perma.cc/TCB3-LFPT].

96 *See* FTC v. Wyndham Worldwide Corp., 799 F.3d 236, 255 (3d Cir. 2015) (noting that the relevant standard under section 5 is "a cost-benefit analysis").

97 *See* Hartzog & Solove, *supra* note 5, at 163.

98 *See, e.g.*, *CISSP® - Certified Information Systems Security Professional*, INT'L INFO. SYS. SEC. CERTIFICATION CONSORTIUM, https://www.isc2.org/cissp/default.aspx [https://perma.cc/FF4C-3PAW] (last visited May 18, 2016).

appropriate data protection practices that a company should adopt to satisfy its duty of care under section 5.

The reasonableness approach is also well suited to the role the FTC plays within the unique data protection framework in the United States. From early on, the United States adopted a mostly self-regulated approach to data privacy, with industry players themselves determining the most effective data protection standards with little congressional regulation in the area.[99] Within this framework, the FTC then assumed the role of a referee, "providing it with oversight and enforcement" and "giv[ing] it legitimacy."[100] The reasonableness approach, with the FTC relying on industry experts to prove unfairness, is not only fully compatible with this framework, but is also one that Congress explicitly envisioned from the very beginning.[101]

As discussed above, Professors Hartzog and Solove go too far in support of the reasonableness approach by arguing that the FTC's settlement documents constitute a reasoned body of law. These documents are not the "functional equivalent of codif[ication]" of industry best data protection practices,[102] and it is expecting too much to find within them sufficient fair notice to satisfy the Due Process Clause. Others, however, go too far in the other direction. Commissioner Wright, for example, has implied that only formal agency regulations can satisfy the fair notice requirement.[103] In district court, Wyndham also asked for formal FTC data protection rules[104] and then argued before the Third Circuit that the

---

99 *See* Solove & Hartzog, *supra* note 11, at 593–94.

100 *Id.* at 598–99.

101 *See* FTC v. R.F. Keppel & Bro., Inc., 291 U.S. 304, 310 n.1 (1934) (quoting Senator Newlands, who stated that "it would be utterly impossible for Congress to define the numerous practices which constitute unfair competition").

102 Hartzog & Solove, *supra* note 5, at 137.

103 *See* Rybnicek & Wright, *supra* note 33, at 1312–13.

104 *See* FTC v. Wyndham Worldwide Corp., 10 F. Supp. 3d 602, 618–19 ("[Wyndham's] arguments boil down to one proposition: the FTC cannot bring an enforcement action under Section 5's unfairness prong without first formally publishing rules and regulations."); *see also* Motion to Dismiss by Defendant Wyndham Hotels & Resorts LLC, *supra* note 13, at 15 ("Because the FTC has not published *any* rules, regulations, or other guidelines explaining what data-security practices the Commission believes Section 5 to forbid or require, it would violate basic principles of fair notice and due process to hold [Wyndham] liable in this case."). Subsequently, Wyndham abandoned this argument on appeal. *See* Appellant's Opening Brief & Joint Appendix Vol. 1, pp. JA1-55 at 39, 45, FTC v. Wyndham Worldwide Corp., 799 F.3d 236 (3d Cir. 2015) (No. 14-3514) (stating that "Wyndham has never disputed the general principle that administrative agencies have discretion to regulate through either rulemaking or adjudication" and that "Wyndham does not contend that 'the FTC would have to cease bringing *all* unfairness actions without first proscribing particularized prohibitions'").

reasonableness standard was not sufficient for fair notice under section 5.[105] These arguments are misplaced because they primarily rest on the inadequacies of the FTC's settlement documents when the pertinent issue is that the reasonableness standard announced in the FTC Act itself provides adequate fair notice.[106] Attempting to shoehorn the Commission's settlement documents into a role for which they were not made does not taint the FTC's entire approach to data protection. To abandon the reasonableness approach in favor of rigid, ineffective rules just because these documents do not provide sufficient notice would be to throw the baby out with the bathwater.

CONCLUSION

Professors Hartzog and Solove's position that settlement agreements and consent decrees constitute the functional equivalent of common law adjudications has fatal flaws—namely that these settlement documents lack the precedential and adversarial values that define common law decisions. Nonetheless, the argument that the FTC cannot bring unfairness claims because it has not provided fair notice completely lacks merit. In lieu of looking to the FTC's settlement documents for fair notice, companies like Wyndham only need to turn to industry professionals and follow the currently accepted best data security practices before breaches occur in order to meet the standard of care the FTC Act requires.[107] Should the Commission ever move away from its referee role and begin enforcing standards inconsistent with those defined by data protection experts, then this fair notice argument may become valid.[108] However, while it continues to apply the reasonableness approach and rely on industry best practices, the FTC properly balances fair notice requirements with its need to remain flexible enough to enforce data protection "in a digital age that is rapidly evolving—and one in which maintaining privacy is, perhaps, an ongoing struggle."[109] In other words, despite the inadequacies of the FTC's settlement documents in providing fair notice, the Commission's data privacy enforcement remains on solid constitutional ground.

---

105 *See* Oral Argument at 16:52, 17:18, FTC v. Wyndham Worldwide Corp., 799 F.3d 236 (3d Cir. 2015) (No. 14-3514), http://www2.ca3.uscourts.gov/oralargument/audio/14-3514FTCv.WyndhamWorldwideCorp,et.al mp3.

106 *See* Rybnicek & Wright, *supra* note 33, at 1304–15.

107 In fact, Wyndham conceded that it hired industry experts after its breaches occurred. *See* Oral Argument, *supra* note 105, at 12:48. The hotel company, however, did not explain why it could not have done so *before* the attacks on its systems.

108 Professors Hartzog and Solove also recognize this possibility. *See* Hartzog & Solove, *supra* note 5, at 163.

109 FTC v. Wyndham Worldwide Corp., 10 F. Supp. 3d 602, 610 (D.N.J. 2014).