Berkeley Technology Law Journal

Volume 31
Issue 2 *Annual Review 2016*

Article 27

9-25-2016

Fair Notice of Unfair Practices: Due Process in FTC Data Security Enforcement after Wyndham

J. William Binkley

Link to publisher version (DOI)
http://dx.doi.org/https://doi.org/10.15779/Z38HC6V

FAIR NOTICE OF UNFAIR PRACTICES: DUE PROCESS IN FTC DATA SECURITY ENFORCEMENT AFTER *WYNDHAM*

J. William Binkley[†]

Section 5 of the Federal Trade Commission Act ("FTC Act") prohibits "unfair or deceptive acts or practices in or affecting commerce" and authorizes the Federal Trade Commission (FTC) to prevent such practices.[1] Since 2002, the FTC has brought more than fifty enforcement actions against businesses for using data security practices that were allegedly unfair or deceptive.[2] Businesses rarely challenged these enforcement actions in court—instead, most settled and entered into consent agreements requiring the company to take certain steps to improve its data security measures. As a result, there had been no explicit ruling on whether the FTC's enforcement of data security exceeded the scope of its Section 5 authority.[3] *FTC v. Wyndham Worldwide Corp.*[4] is the first case to directly address this question.

In 2012, the FTC sued the Wyndham Hotels chain following a data breach in which hackers obtained the financial information of thousands of Wyndham customers.[5] Wyndham moved to dismiss the complaint, arguing that its conduct was not unfair, that the FTC lacked authority to regulate

DOI: http://dx.doi.org/10.15779/Z389857

† J.D. Candidate, 2017, University of California, Berkeley, School of Law.

1. 15 U.S.C. § 45(a) (2012) (codifying Section 5 of the FTC Act).

2. *See* FED. TRADE COMM'N, COMMISSION STATEMENT MARKING THE FTC'S 50TH DATA SECURITY SETTLEMENT (Jan. 31, 2014), https://www.ftc.gov/system/files/documents/cases/140131gmrstatement.pdf [https://perma.cc/Y8Z2-HSAU] (announcing the FTC's fiftieth data security settlement in enforcement actions brought under its authority to "protect[] consumers from deceptive and unfair commercial practices").

3. *See, e.g.*, *In re* BJ's Wholesale Club, Inc., 140 F.T.C. 465 (2005) (consent order based on unfair trade practices); *In re* Twitter, Inc., 151 F.T.C. 162 (2011) (consent order based on deceptive trade practices).

4. 799 F.3d 236 (3d Cir. 2015). In one other case, the respondent in an administrative proceeding sued in district court to challenge the FTC's data security enforcement authority, but the case was dismissed on jurisdictional grounds. *See* LabMD, Inc. v. FTC, 776 F.3d 1275, 1277 (11th Cir. 2015) (upholding the district court's dismissal of LabMD's complaint).

5. *See* First Amended Complaint for Injunctive and Other Equitable Relief at 17–19, FTC v. Wyndham Worldwide Corp., No. 12-cv-1365 (D. Ariz. Aug. 9, 2012).

data security under Section 5, and that Wyndham had not been given fair notice of the particular data security standards it was required to meet. On appeal, the Third Circuit affirmed the district court's dismissal of the motion.[6] Wyndham has since settled charges with the FTC.[7]

This result generally supports the approach the FTC has taken in targeting inadequate data security as an "unfair" commercial practice under Section 5. The case raises important questions, however, about the fair notice issue. Due process requires that defendants—whether in a criminal, civil, or administrative proceeding—be given fair notice of what the law requires. And the fair notice standard is more stringent in cases where an administrative agency acts under its own interpretation of a statute. Circuit courts have defined this as the "ascertainable certainty" standard: regulated parties must be able to ascertain what conduct is required or prohibited under an agency's interpretation.[8]

Some scholars have argued that the FTC's past data security complaints and consent orders form a body of "common law" that defines data security practices the agency considers to be unfair or deceptive.[9] Others have argued that these complaints and consent orders are arbitrary and provide little guidance to companies trying to avoid liability.[10] Against this backdrop, the

6. *Wyndham*, 799 F.3d at 259.

7. *See* Stipulated Order for Injunction at 1–2, FTC v. Wyndham Worldwide Corp., No. 13-1887 (D.N.J. Dec. 11, 2015).

8. *See, e.g.*, Sec'y of Labor v. Beverly Healthcare-Hillview, 541 F.3d 193, 202 (3d Cir. 2008); Gen. Elec. Co. v. EPA, 53 F.3d 1324, 1329 (D.C. Cir. 1995); Georgia Pac. Corp. v. Occupational Safety & Health Review Comm'n, 25 F.3d 999, 1005 (11th Cir. 1994).

9. *See, e.g.*, Daniel J. Solove & Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, 114 COLUM. L. REV. 583, 608 (2014) ("FTC enforcement has certainly changed over the course of the past fifteen years, but the trajectory of development has followed a predictable set of patterns . . . . [W]e argue that the body of FTC settlements is the functional equivalent of privacy common law."); Christopher Wolf, *Targeted Enforcement and Shared Lawmaking Authority As Catalysts for Data Protection in the United States*, 15 ELECTRONIC COM. & L. REP. (BNA) No. 47, 58 (Dec. 15, 2010) ("FTC enforcement . . . has created a 'common law of consent decrees,' producing a set of data protection rules for businesses to follow.").

10. *See, e.g.*, Gerard M. Stegmaier & Wendell Bartnick, *Physics, Russian Roulette, and Data Security: The FTC's Hidden Data-Security Requirements*, 20 GEO. MASON L. REV. 673, 719 (2013) ("Entities have not been given proper notice of what data-security practices are 'reasonable' and 'adequate'" and thus "have little hope of confidently ensuring that they have successfully complied with Section 5."); Michael D. Scott, *The FTC, the Unfairness Doctrine, and Data Security Breach Litigation: Has the Commission Gone Too Far?*, 60 ADMIN. L. REV. 127, 183 (2008) (arguing that FTC data security complaints are "seemingly filed at random, without any guidelines, and without any advance notice to the respondents that their actions might violate Section 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)" in the data security realm.).

Wyndham decision's treatment of the fair notice issue is somewhat unclear. The Third Circuit's analysis suggested that past complaints and guidelines could provide notice of what practices the FTC interprets to be unfair, but it held that Wyndham had notice based solely on the statute, regardless of any interpretation by the FTC.

This Note argues that courts should analyze fair notice in FTC data security cases according to a three-part framework: (1) past complaints and guidelines can provide "ascertainable certainty" of the FTC's interpretation where they identify the same pattern of alleged conduct; (2) consent orders do not satisfy the fair notice requirement but may still provide useful guidance to companies; and (3) where past complaints and guidelines do not cover the alleged conduct in a case, courts should look to the statute without reference to FTC interpretation, and a less stringent fair notice standard should apply. The Note begins with an overview of the FTC's general rulemaking and enforcement authority, the history of FTC data security enforcement, and the fair notice doctrine as it applies to administrative agency enforcement. Part II describes the facts, procedural history, and reasoning of the *Wyndham* case in more detail. Part III argues that although the Third Circuit reached the correct conclusion, the court's analysis of the fair notice issue is somewhat unclear; it then goes on to outline the three-part framework.

I. BACKGROUND

In order to analyze the significance of the Third Circuit's holding in *Wyndham*, it is important to understand the FTC's general statutory authority to regulate unfair and deceptive trade practices, and how the agency has exercised this authority in the data security context. This Part will also address the fair notice doctrine, in general and as it applies to agency interpretations, to assess Wyndham's fair notice arguments.

A. THE FTC'S ENFORCEMENT AUTHORITY

The broad language of the FTC Act gives the Commission significant authority to prevent unfair and deceptive practices that injure consumers. Although the FTC can create regulations that define particular acts as unfair or deceptive, it rarely does so because the rulemaking procedure is so burdensome; instead, the agency typically files complaints alleging a violation of the statute rather than a violation of any regulation.

1. Statutory Authority Under Section 5 of the FTC Act

The FTC Act gives the Commission authority to regulate a broad range of commercial activity in order to protect consumers from "unfair or deceptive acts or practices."[11] Section 5(a) of the FTC Act provides that:

> (1) Unfair methods of competition in or affecting commerce, and unfair or deceptive acts or practices in or affecting commerce, are hereby declared unlawful.
>
> (2) The Commission is hereby empowered and directed to prevent persons, partnerships, or corporations . . . from using unfair methods of competition in or affecting commerce and unfair or deceptive acts or practices in or affecting commerce.[12]

The history of the statute over the past century is one of significant expansion.[13] Congress created the Commission in 1914 as an antitrust enforcement agency.[14] The 1938 Wheeler-Lea Act[15] later gave the agency authority to regulate consumer protection issues beyond the area of competition. In 1975, the Magnuson-Moss Warranty-Federal Trade Commission Improvement Act ("Magnuson-Moss") further expanded the FTC's jurisdiction to cover unfair or deceptive acts or practices, and unfair methods of competition, in commerce "*or affecting* commerce."[16] Magnuson-Moss also provided a rulemaking process through which the FTC could issue regulations to define specific acts as unfair or deceptive.[17]

The FTC has faced a number of legal challenges to the scope of its Section 5 enforcement authority, and the outcome of these cases further established the wide reach of the agency's regulatory powers. "Unfair" methods and practices may be defined broadly and are not limited to any

11. *See* 15 U.S.C. § 45(a); *see also* STEPHANIE W. KANWIT, 1 FEDERAL TRADE COMMISSION 1:1 (2015) (describing the FTC's mandate as "broader in scope than that of any other governmental agency" and affecting "virtually every business in the country, from local furniture stores to 'Fortune 500' corporations").

12. § 45(a).

13. *See generally* CHRIS JAY HOOFNAGLE, FEDERAL TRADE COMMISSION PRIVACY LAW AND POLICY 3–81 (2016) (describing the FTC's growth as a series of "pivots" and reactions as the agency's jurisdiction expanded).

14. 38 Stat. 719 (1914) (prohibiting "unfair methods of competition in commerce").

15. 52 Stat. 111 (1938) (adding language prohibiting "unfair or deceptive acts or practices").

16. Pub. L. No. 93-637, 88 Stat. 2183 (1975) (emphasis added). Magnuson-Moss is codified at 15 U.S.C. §§ 57a, 2301–2312 (2012).

17. *See* § 57a(a)–(b).

set of specifically prohibited acts.[18] Likewise, the FTC can consider public policies other than competition in defining what is an unfair or deceptive act or practice.[19]

Section 5(n) of the FTC Act, added in 1994, imposes an important limitation on FTC enforcement authority. It provides that the FTC may not find an act or practice to be unfair or deceptive "unless the act or practice *causes or is likely to cause substantial injury* to consumers which is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition."[20] The FTC may consider public policy when determining whether a practice is unfair, but "[s]uch public policy considerations may not serve as a primary basis for such determination."[21] Under Section 5, therefore, an act or practice can only be unfair or deceptive if it is unreasonable in balancing harms and benefits.

2. The FTC's Use of Rulemaking Processes

Congress has granted the FTC the authority to create and enforce regulations in support of the agency's mission. To promulgate a new regulation, the FTC must go through the steps of a rulemaking process prescribed by Congress. The process varies according to the particular

18. *See* FTC. v. R.F. Keppel & Bro., Inc., 291 U.S. 304, 314 (1934) ("It is unnecessary to attempt a comprehensive definition of the unfair methods which are banned, even if it were possible to do so . . . . New or different practices must be considered as they arise in the light of the circumstances in which they are employed."); *see also* Sears, Roebuck & Co. v. FTC., 258 F. 307, 311–12 (7th Cir. 1919) (finding that, by using the general term "unfair methods" without defining it, Congress charged the FTC with determining what specific acts fit the definition).

19. *See* FTC v. Sperry & Hutchinson Co., 405 U.S. 233, 239 (1972) (Section 5 "empower[s] the Commission to proscribe practices as unfair or deceptive in their effect upon consumers regardless of their nature or quality as competitive practices or their effect on competition.").

20. 15 U.S.C. § 45(n) (2012) (emphasis added). Substantial injury can arise from an "act or practice" that causes a "small harm to a large number of people, or if it raises a significant risk of concrete harm." FTC v. Neovi, Inc., 604 F.3d 1150, 1157 (9th Cir. 2010) (quoting Am. Fin. Servs. Ass'n v. FTC, 767 F.2d 957, 972 (D.C. Cir. 1985)).

21. § 45(n). In effect, Section 5(n) codified a limit on the definition of "unfairness" that the Commission had articulated in a 1980 policy statement. *See* Letter from Michael Pertschuk, Chairman, Fed. Trade Comm'n to Wendell H. Ford, Chairman, and John C. Danforth, Ranking Minority Member, S. Comm. on Commerce, Science, and Transp. (Dec. 17, 1980), *appended to* Int'l Harvester Co., 104 F.T.C. 949, 1070–76 (1984) ("To justify a finding of unfairness the injury must satisfy three tests. It must be substantial; it must not be outweighed by any countervailing benefits to consumers or competition that the practice produces; and it must be an injury that consumers themselves could not reasonably have avoided.").

statute under which the agency is operating, however, and the FTC must follow an especially burdensome process to promulgate regulations under Section 5. As a result, the FTC virtually never uses the rulemaking process to define particular acts and practices as unfair or deceptive.

In some instances, Congress directs the FTC to follow the notice-and-comment rulemaking procedures set forth in the Administrative Procedure Act ("APA") when promulgating new regulations.[22] As discussed in Section I.B.1 below, the Gramm-Leach-Bliley Act ("GLBA")[23] authorized the FTC to create rules, following APA notice-and-comment procedures, to govern certain financial institutions' use of customers' personal information.[24] Likewise, the Children's Online Privacy Protection Act ("COPPA")[25] required the FTC to promulgate regulations concerning online services' use of children's personal information, again following the APA's notice-and-comment rulemaking procedures.[26]

But if the FTC wishes to promulgate a regulation under Section 5 of the FTC Act—that is, to "define with specificity acts or practices which are unfair or deceptive"—the Magnuson-Moss Act requires the Commission to follow a more burdensome rulemaking process.[27] In addition to the notice-and-comment requirements of the APA, the FTC must provide additional notice at several stages: advance notice to House and Senate committees; advance notice in the Federal Register of "the area of inquiry under consideration, the objectives which the Commission seeks to achieve, and possible regulatory alternatives;" and a notice with the full text of the

22. *See* 5 U.S.C. § 553 (2012). The APA requires that an agency seeking to make a new rule publish a notice of proposed rulemaking that states the time, place, and nature of the rulemaking proceedings; the legal authority for the proposed regulation; and "either the terms or substance of the proposed rule or a description of the subjects and issues involved." *Id.* § 553(b). The agency must give the public an opportunity to submit "written data, views, or arguments." *Id.* § 553(c). After considering public comments, the agency must publish the final rule in the Federal Register with a "concise general statement of [the rule's] basis and purpose." *Id.*

23. Pub. L. No. 106-102, 113 Stat. 1338 (1999). The Gramm-Leach-Bliley Act is codified at 15 U.S.C. §§ 6801–6809, 6821–6827.

24. *See* § 6804(a).

25. Pub. L. No. 105-277, 112 Stat. 2681-728 (1998). The Children's Online Privacy Protection Act is codified at 15 U.S.C. §§ 6501–6506.

26. *See* § 6502(b)(1) (requiring the FTC to "promulgate regulations under section 553 of title 5").

27. *See generally id.* § 57a; FED. TRADE COMM'N, OPERATING MANUAL § 7, https://www.ftc.gov/sites/default/files/attachments/ftc-administrative-staff-manuals/ch07rulemaking.pdf [https://perma.cc/NBA3-QQ3S] (describing the rulemaking process in detail).

proposed rule including any alternatives.[28] The FTC must also determine that the regulated activity is "prevalent"[29] and must hold a hearing and give interested parties, at a minimum, the opportunity to be heard and to present evidence.[30] Once the agency promulgates a Magnuson-Moss regulation, it must publish statements regarding the "prevalence of the acts or practices," the "manner and context in which such acts or practices are unfair or deceptive," and the "economic effect of the rule."[31] Interested parties may also challenge the regulation in court; a judge must vacate the rule if it is not supported by "substantial evidence in the rulemaking record" or if limits on cross-examination prevented the disclosure of "disputed material facts . . . necessary for [a] fair determination."[32]

Because the Magnuson-Moss rulemaking process is so lengthy and cumbersome, it is rarely used.[33] Instead of promulgating new regulations to define particular acts and practices as unfair or deceptive, the FTC can bring enforcement actions under the language of the statute. The APA explicitly makes an exception to the notice-and-comment rules for "interpretative rules, general statements of policy, or rules of agency organization, procedure, or practice."[34] Thus, agencies may state their own policies and procedures, and state what they believe a statute already requires or forbids, without going through the rulemaking process. At the FTC, these interpretations can take the form of official policy statements, industry guidelines, public reports, or advisory opinions.[35] Unlike regulations,

28. § 57a(b).

29. *See id.* § 57a(b)(3).

30. *See id.* § 57a(c) (providing interested parties the opportunity to be heard and the possibility of cross-examining witnesses in certain circumstances).

31. *Id.* § 57a(d).

32. *Id.* § 57a(e).

33. *See* Solove & Hartzog, *supra* note 9, at 620 (describing the Magnuson-Moss rulemaking process as "largely ineffective"); *America's Top Consumer Protection Cop Needs Better Weapons in its Arsenal*, CTR. FOR DEMOCRACY & TECH. (Feb. 5, 2010), https://cdt.org/blog/america%E2%80%99s-top-consumer-protection-cop-needs-better-weapons-in-its-arsenal [https://perma.cc/2XMK-5TR3] ("The FTC cannot adequately respond to conduct in the marketplace that harms consumers by crafting rules that take 8–10 years to promulgate . . . . [A]s a result, the FTC regularly avoids Magnuson-Moss rulemaking altogether.").

34. 5 U.S.C. § 553(b)(3)(A) (2012). On one occasion when the FTC did engage in Magnuson-Moss rulemaking, the agency received over 20,000 pages of public comments and generated an additional 18,000 pages of transcripts and exhibits over fifty-two days of hearings—the process began in 1972 but did not produce a final rule until 1984. *See* Harry & Bryant Co. v. FTC, 726 F.2d 993, 996 (4th Cir. 1984).

35. *See generally* FED. TRADE COMM'N, OPERATING MANUAL § 8, https://www.ftc.gov/sites/default/files/attachments/ftc-administrative-staff-manuals/ch08industryguidance.pdf

however, agency interpretations do not have the force of law—an agency bringing an enforcement action must plead a violation of the underlying statute rather than a violation of that particular interpretation.[36]

3. Enforcement Procedures at the FTC

The FTC has two possible avenues for bringing an enforcement action under Section 5 of the FTC Act: administrative trials and judicial enforcement in a federal district court. Filing a complaint in federal court is somewhat more common, since it allows the FTC to seek permanent injunctions to prevent future conduct by the defendant, but each approach has its own procedural and strategic advantages.

Under Section 5(b), the Commission may file an administrative complaint against a person or entity if there is "reason to believe" it has engaged in an unfair or deceptive act or practice, and if it appears the proceeding would be in the public interest.[37] The commissioners must vote on whether to issue a complaint.[38] When a complaint has been filed, the respondent may elect to settle the charges, agree to the entry of a final order, and waive the right to judicial review.[39] If the respondent chooses instead to contest the complaint, the dispute is adjudicated in a hearing before an administrative law judge (ALJ), who makes an initial decision on the case.[40] Either the respondent or the FTC may appeal the ALJ's decision to the full Commission; the parties then have the opportunity to submit briefs and give oral argument before the commissioners.[41] Once the Commission enters a final decision, the respondent may petition a circuit court for review of the order.[42] The administrative process can only result in a cease-and-desist order, however, so the Commission may not impose other penalties when it issues a final order.[43] If a respondent has knowingly violated a final cease-

[https://perma.cc/5Y3M-PSB8] (discussing the scope, characteristics, and procedures of various forms of guidance the FTC provides).

36. *See id.* § 8.3.2.

37. 15 U.S.C. § 45(b).

38. 16 C.F.R. § 3.11(a) (2015).

39. *See A Brief Overview of the Federal Trade Commission's Investigative and Law Enforcement Authority*, FED. TRADE COMM'N (July 2008), https://www.ftc.gov/about-ftc/what-we-do/enforcement-authority [https://perma.cc/Q7LV-6MXK] (describing the FTC's administrative and judicial enforcement procedures).

40. *Id.*

41. *Id.*

42. 15 U.S.C. § 45(c).

43. *See id.* § 45(b).

and-desist order, then the FTC may bring a civil suit in district court seeking a monetary penalty or other equitable relief for the violation.[44]

The administrative process is somewhat shorter where the FTC is enforcing a regulation it has issued through notice-and-comment or Magnuson-Moss rulemaking. The FTC may file a complaint in district court for the violation of a rule without first conducting hearings before an ALJ or the full Commission.[45] If the court finds that the defendant has violated a rule, it may impose monetary penalties or other equitable relief, just as it would for violation of a cease-and-desist order.[46] Thus, the rulemaking process can be an alternative to pursuing cease-and-desist orders against individual respondents through administrative hearings.

Alternatively, the FTC can seek judicial enforcement for violation of the FTC Act by filing a civil suit directly with a federal district court. The Commission must have reason to believe that a "person, partnership, or corporation is violating, *or is about to violate*" a law enforced by the FTC and that such a proceeding would be in the public interest.[47] Judicial enforcement proceedings can therefore target prospective violations as well as past conduct, and a court may order a permanent injunction as a remedy.[48] Because of the advantages this approach offers, "most consumer protection enforcement is now conducted directly in court . . . rather than by means of administrative adjudication."[49] Nevertheless, there are advantages to using the administrative process instead. In an administrative hearing, the FTC "has the first opportunity to make factual findings and articulate the relevant legal standard," and a court reviewing a final decision by the Commission must give "substantial deference" to the FTC's interpretation.[50]

B. FTC ENFORCEMENT IN THE DATA SECURITY CONTEXT

The FTC's authority to regulate data security stems from two sources: specific data security legislation and its general authority under Section 5 to regulate "unfair or deceptive" acts and practices. Importantly, the FTC has not engaged in the rulemaking process to promulgate data security

44. *Id.* § 45(l).

45. *Id.* § 45(m); *see also* FED. TRADE COMM'N, *supra* note 39 (describing the enforcement of promulgated trade regulations "[i]n lieu of administrative adjudications against individual respondents").

46. § 45(m).

47. 15 U.S.C. § 53(b) (2012) (emphasis added).

48. *Id.*

49. FED. TRADE COMM'N, *supra* note 39.

50. *Id.* (noting that, as a result, "where a case involves novel legal issues or fact patterns, the Commission has tended to prefer administrative adjudication").

regulations under Section 5. Because the agency has not issued regulations to define specifically what practices are required or prohibited, its regulation of unfair and deceptive data security practices rests on its interpretation of the broad language of the statute.

1. Sector-Specific Data Security Statutes

Congress has enacted several statutes that provide for FTC regulation of data security within specific areas. The 1999 GLBA[51] stated that Congress's policy in enacting the legislation was to ensure "that each financial institution has an affirmative and continuing obligation to respect the privacy of its customers and to protect the security and confidentiality of those customers' nonpublic personal information."[52] The statute required a number of agencies, including the FTC, to set standards that financial institutions must meet to safeguard the confidentiality of customer records, protect the security and integrity of such records, and protect against unauthorized access or use.[53] The FTC has issued a Safeguards Rule under the statute that defines more specifically the standards for financial institutions under the agency's jurisdiction.[54]

COPPA is a privacy and data protection statute that applies to the operators of websites and other online services "who collect[] or maintain[] personal information" of children under the age of thirteen.[55] Like GLBA, COPPA required the FTC to create a rule for regulated entities to follow. Specifically, it directed the FTC to promulgate regulations prohibiting online service operators from collecting children's personal information without providing notice and obtaining parental consent.[56] The FTC's COPPA Rule details with more specificity the standards that online services must meet, including "establish[ing] and maintain[ing] reasonable procedures to protect the confidentiality, security, and integrity of personal information collected from children" and taking "reasonable steps to release children's personal information only to service providers and third parties

51. 15 U.S.C. §§ 6801–6809, 6821–6827 (2012).
52. *Id.* § 6801(a).
53. *Id.* § 6801(b).
54. *See generally* 16 C.F.R. § 314 (2015). The regulation requires financial institutions to "develop, implement, and maintain a comprehensive information security program" that includes "reasonably designed" safeguards, and it identifies several elements that data security programs must meet. *Id.* § 314.3–314.4.
55. 15 U.S.C. § 6501 (2012).
56. 15 U.S.C. § 6502(b)(1)(A) (2012).

who are capable of maintaining the confidentiality, security and integrity of such information."[57]

The Fair Credit Reporting Act ("FCRA")[58] also delegates data security enforcement authority to the FTC within a particular area. FCRA governs the use and disclosure of credit reports, and it requires credit-reporting agencies to follow "reasonable procedures" for protecting the "confidentiality, accuracy, relevancy, and proper utilization" of consumer credit information.[59] Congress gave the FTC authority to enforce compliance with the statute, including against violators who would otherwise not satisfy the jurisdictional requirements of the FTC Act.[60]

These statutes and their accompanying regulations clearly direct the FTC to enforce data security requirements within certain domains. The scope of specific legislation is limited, however, to the narrow areas defined in each statute. Congress has never passed legislation to require general data security or privacy protections outside these narrow areas, although such legislation has been proposed on numerous occasions.[61] The FTC has also recommended that Congress enact broader data security legislation and give the agency additional rulemaking authority.[62]

57. 16 C.F.R. § 312.8 (2015).

58. 15 U.S.C. §§ 1681–1681x (2012).

59. *Id.* § 1681(b).

60. *See id.* § 1681s(a)(1) (providing that "a violation of any requirement or prohibition imposed under this subchapter shall constitute an unfair or deceptive act or practice . . . irrespective of whether that person is engaged in commerce or meets any other jurisdictional tests under the Federal Trade Commission Act").

61. *See, e.g.*, Data Security Act of 2015, S. 961, 114th Cong. (2015) (proposing to establish "uniform national data security and breach notification standards for electronic data"); Data Security and Breach Notification Act of 2015, S. 177, 114th Cong. (2015) (seeking to "protect consumers by requiring reasonable security policies and procedures to protect data containing personal information, and to provide for nationwide notice in the event of a breach of security"); Consumer Privacy Protection Act of 2015, S. 1158, 114th Cong. (2015) (proposing a regulatory system to protect "against security breaches, fraudulent access, and misuse of personal information"). Similar bills were also introduced in prior years but none have been enacted. *See, e.g.*, Data Security and Breach Notification Act of 2014, S. 1976, 113th Cong. (2014); Personal Data Privacy and Security Act of 2014, S. 1897, 113th Cong. (2014).

62. *See* FED. TRADE COMM'N, DATA BREACH ON THE RISE: PROTECTING PERSONAL INFORMATION FROM HARM, at 9–11 (Apr. 2, 2014) (recommending, to the U.S. Senate Committee on Homeland Security and Governmental Affairs, data security legislation that would expand the FTC's jurisdiction and grant it APA rulemaking authority in the area of data security).

2. Enforcement Actions the FTC Has Brought Under Section 5

In areas that do not fall within the sector-specific statutes described above, the FTC conducts its data security enforcement under the general language of Section 5. The agency has filed numerous complaints characterizing certain data security practices as "unfair" or "deceptive," and the vast majority of these enforcement actions have resulted in settlements and entries of consent orders. As demonstrated below, the content of complaints and consent orders differs in important ways.

Since 2002, the FTC has brought more than fifty such enforcement actions for allegedly unfair or deceptive data security practices under Section 5. The earliest cases operated under the "deception" prong of the statute: the FTC argued, for example, that Microsoft's privacy policy related to its .NET Passport service misrepresented the level of security protecting user data.[63] More recently, the FTC has targeted data security practices as "unfair"—in such cases, the FTC has argued that lax security measures unfairly put personal information at risk, whether or not the company deceived consumers by publishing a misleading privacy policy.[64]

A deceptive act or practice can also be unfair, and the FTC in some cases has argued that a defendant's conduct violated both prongs. In *Wyndham*, for example, the FTC alleged both that Wyndham misrepresented the strength of its data security measures and that the company's failure to employ "reasonable and appropriate measures to protect personal information" was unfair.[65]

These cases, whether premised on deception or unfairness, have overwhelmingly resulted in settlement and the entry of a consent order, without adjudication on the merits. The content of these consent orders varies from case to case; typically, however, they require the defendant to

63. *In re* Microsoft Corp., 134 F.T.C. 709, 711–12 (2002) ("[Microsoft] represented, expressly or by implication, that it maintained a high level of online security by employing sufficient measures reasonable and appropriate under the circumstances to maintain and protect the privacy and confidentiality of personal information obtained from or about consumers . . . . In truth and in fact, [Microsoft] did not maintain a high level of online security.").

64. *See, e.g.*, *In re* BJ's Wholesale Club, Inc., 140 F.T.C. 465, 466–68 (2005) (complaint alleging that failure to secure in-store wireless network when transmitting customer credit card information, together with other security failures, was an unfair practice); *In re* DSW Inc., 141 F.T.C. 117, 119–20 (2006) (complaint alleging that use of unencrypted files on insecure network, together with other security failures, was an unfair practice).

65. First Amended Complaint for Injunctive and Other Equitable Relief at 18–19, FTC v. Wyndham Worldwide Corp., No. 12-cv-1365 (D. Ariz. Aug. 9, 2012).

implement reasonable data security measures and to comply with monitoring and reporting requirements for a fixed period of time.[66] Companies often have strong incentives to settle after a complaint is filed, rather than fight in an administrative or judicial proceeding: settlement allows companies to avoid admitting liability, and the price of settling may be less than the costs of litigation.[67]

Comparing a typical FTC complaint with a consent order helps to illustrate the way in which each type of document might provide notice of the agency's interpretation of what the statute requires. In 2010, the FTC filed an administrative complaint against Dave & Busters, Inc.[68] The complaint alleged that the company's unfair data security practices had allowed hackers to access customer credit card information.[69] Specifically, it alleged that the following practices, taken together, were unfair: (1) failure to use sufficient measures to detect, prevent, and investigate unauthorized network access; (2) failure to limit third-party access to networks; (3) failure to identify and block unauthorized personal information exported from the network; (4) failure to use "readily available" means such as firewalls to isolate the card payment system or limit access between networks in the store; and (5) failure to use "readily available" means to limit wireless network access.[70]

Dave & Buster's settled and entered into an agreement and consent order with the FTC but admitted no liability.[71] The consent order required the company to "establish and implement, and thereafter maintain, a comprehensive information security program . . . contain[ing] administrative, technical, and physical safeguards appropriate to respondent's size and complexity, the nature and scope of respondent's activities, and the sensitivity of the personal information collected from or about consumers."[72] The data security program was to include (1) a designated employee to coordinate the program; (2) a risk assessment; (3) "the design and implementation of reasonable safeguards" to address those risks; (4) development of a system to ensure that service providers safeguarded personal information; and (5) adjustments to the program in light of any

66. *See, e.g.*, BJ's Wholesale Club, 140 F.T.C. at 470–75 (requiring implementation of a data security program "reasonably designed to protect the security, confidentiality, and integrity of personal information collected from or about consumers").

67. *See* Solove & Hartzog, *supra* note 9, at 611–13.

68. *See In re* Dave & Buster's, Inc., 149 F.T.C. 1449 (2010).

69. *Id.* at 1451–52.

70. *Id.* at 1451.

71. *Id.* at 1453.

72. *Id.* at 1455.

future developments or circumstances.[73] The order further required Dave & Buster's to obtain and submit regular reports on its data security program from a "qualified, objective, independent third-party professional," and to comply with other reporting requirements for a period of ten years.[74]

Several differences are apparent between the allegations of the complaint and the requirements of the consent order. The complaint identified specific data security failures—failure to monitor networks, use firewalls, protect wireless access, etc.—that were allegedly a violation of Section 5 when taken as a whole. The consent order, on the other hand, imposed more general requirements, including the development and implementation of a security program, reporting duties, and certification by a third-party professional. This type of remedy, known as "fencing-in relief," imposes additional duties beyond merely ceasing and desisting from the conduct alleged in the complaint.[75] The consent order also contains no allegation or admission that the company's past data security practices actually violated the statute. Because it alleges no violation, mandates additional conduct beyond ceasing the practices alleged in the complaint, and is limited to the party involved, the consent order provides little guidance about what data security practices the FTC actually requires. Again, the contents of this complaint and consent order are typical of most FTC data security enforcement actions.

3. Other Forms of Data Security Guidance Issued by the FTC

In addition to the complaints and consent orders that emerge from enforcement actions, the FTC has published data security guidelines and other documents that can shed light on the agency's understanding of what practices are unfair under Section 5.

Several FTC guidebooks offer data security advice. The 2015 Start with Security guide, for example, outlines ten security principles that "touch on vulnerabilities that could affect [a] company, along with practical guidance on how to reduce the risks they pose."[76] These principles are "[d]istill[ed]" from FTC cases and advise companies to use secure passwords and authentication, encrypt data in transmission and at rest, and monitor

73. *Id.* at 1455–56.

74. *Id.* at 1456–57.

75. *See* FTC v. National Lead Co., 352 U.S. 419, 431 (1957) ("[T]hose caught violating the [FTC] Act must expect some fencing in.").

76. FED. TRADE COMM'N, START WITH SECURITY: A GUIDE FOR BUSINESS 1 (2015), https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf [https://perma.cc/X32U-CG6B].

network access, among other measures.[77] Likewise, the 2011 Protecting Personal Information guide provides "checklists" that companies can follow in creating a data security plan.[78] The guide is structured around five "key principles" for keeping data secure.[79] The guide includes more detailed advice under each principle, such as "[i]f some computers on your network store sensitive information while others do not, consider using additional firewalls to protect the computers with sensitive information."[80] Other reports the FTC has published include similar guidance.[81]

In sum, then, there are three categories of documents that might provide notice of the FTC's interpretation of what particular data security practices violate Section 5: complaints, consent orders, and other published guidelines. This Note will next discuss the fair notice doctrine—both as a general constitutional requirement and as the doctrine applies to federal agency interpretations of a statute—to lay the groundwork for analyzing the extent to which each category of document may satisfy the fair notice requirement.

C. THE FAIR NOTICE DOCTRINE

The fair notice standard that a court will apply depends on the context. A stricter fair notice standard applies in criminal cases, and a less strict standard applies in cases involving civil penalties and economic regulation.[82]

---

77. *Id.* at 1–8.

78. FED. TRADE COMM'N, PROTECTING PERSONAL INFORMATION: A GUIDE FOR BUSINESS 3 (Nov. 2011), https://www.ftc.gov/system/files/documents/plain-language/bus69-protecting-personal-information-guide-business_0.pdf [https://perma.cc/9HRY-WC2C]. The Third Circuit in *Wyndham* cited an earlier edition of this guidebook, noting that the guide "counsel[ed] against many of the specific practices alleged here." FTC v. Wyndham Worldwide Corp., 799 F.3d 236, 256 (3d Cir. 2015).

79. FED. TRADE COMM'N, *supra* note 78, at 3 ("1. Take stock. Know what personal information you have in your files and on your computers. 2. Scale down. Keep only what you need for your business. 3. Lock it. Protect the information that you keep. 4. Pitch it. Properly dispose of what you no longer need. 5. Plan ahead. Create a plan to respond to security incidents.").

80. *Id.* at 15.

81. *See, e.g.*, FED. TRADE COMM'N, INTERNET OF THINGS: PRIVACY & SECURITY IN AN INTERCONNECTED WORLD (Jan. 2015), https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf [https://perma.cc/TFY3-P3QF] (staff report summarizing FTC recommendations for securing data in networked consumer devices); FED. TRADE COMM'N, MOBILE APP DEVELOPERS: START WITH SECURITY (Feb. 2013), https://www.ftc.gov/tips-advice/business-center/guidance/mobile-app-developers-start-security [https://perma.cc/366T-96VU] (offering guidance for implementing "reasonable data security" in mobile applications).

82. *See infra* Section I.C.1.

Where an agency is enforcing its own interpretation of a statute, however—even if it concerns economic regulation—this moves the analysis back to a stricter standard.[83]

1. Due Process Includes a General Right to Fair Notice

As a constitutional matter of due process, defendants are entitled to "fair notice" that their conduct may subject them to liability.[84] The level of notice required in a particular case falls along a spectrum: the requirement is stricter when criminal penalties are imposed and less strict in cases involving civil penalties or economic regulation.

In criminal law, a statute violates due process if it "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."[85] There is a concern that "[v]ague laws may trap the innocent" without warning or "impermissibly delegate[] basic policy matters" to law enforcement, judges, and juries.[86] Fair notice principles also apply to civil statutes, but courts are more tolerant of vagueness where the consequences are less severe than criminal penalties.[87] And economic regulation is "subject to a less strict vagueness test because its subject matter is often more narrow, and because businesses . . . can be expected to consult relevant legislation in advance of action."[88] When an agency enforces a civil statute concerning economic regulation, therefore, the applicable fair notice standard is quite deferential.[89]

---

83. *See infra* Section I.C.2.

84. *See* FCC v. Fox Television Stations, 132 S. Ct. 2307, 2317 (2012) ("A fundamental principle in our legal system is that laws which regulate persons or entities must give fair notice of conduct that is forbidden or required.").

85. United States v. Williams, 553 U.S. 285, 304 (2008) (citing Hill v. Colorado, 530 U.S. 703, 732 (2000)).

86. Grayned v. City of Rockford, 408 U.S. 104, 108–09 (1972).

87. *See* Vill. of Hoffman Estates v. Flipside, Hoffman Estates, Inc., 455 U.S. 489, 498–99 (1982) (noting that the Supreme Court has "expressed greater tolerance with civil rather than criminal penalties because the consequences of imprecision are qualitatively less severe").

88. *Id.* at 498.

89. *See* United States v. Midwest Fireworks Mfg. Co., 248 F.3d 563, 568 (6th Cir. 2001) ("[Economic] statutes and regulations will not become impermissibly vague simply because it may be difficult to determine whether marginal cases fall within their scope.") (internal quotation marks omitted); Ass'n of Int'l Auto. Mfrs., Inc. v. Abrams, 84 F.3d 602, 614 (2d Cir. 1996) ("A civil statute is not impermissible under this [notice] standard unless its commands are 'so vague and indefinite as really to be no rule or standard at all.'") (quoting Boutilier v. INS, 387 U.S. 118, 123 (1967)); United States v. Sun & Sand Imports, Ltd., Inc., 725 F.2d 184, 188 (2d Cir. 1984) (noting that "[o]nly a reasonable degree of certainty is necessary" in economic regulation).

2. *A Stricter Fair Notice Standard of "Ascertainable Certainty" Applies to Agency Interpretations*

A stricter standard applies, however, when an agency has issued a particular interpretation of a statute and acts under that interpretation. Several circuit courts have termed this the "ascertainable certainty" standard: fair notice exists "[i]f, by reviewing the regulations and other public statements issued by the agency, a regulated party acting in good faith would be able to identify, with 'ascertainable certainty,' the standards with which the agency expects parties to conform."[90] An agency's statement that it has adopted a particular interpretation can take various forms, but it must be "publicly accessible" and not merely private or informal.[91] In effect, agency interpretation takes the fair notice analysis out of the deference that usually applies to economic regulation and moves it closer to the strict standard that applies in criminal cases.[92]

Two examples will help illustrate the situations in which courts are likely to find that an agency's interpretation has not provided adequate notice. In *FCC v. Fox Television Stations, Inc.*, the Supreme Court held that the FCC had not given television broadcasters fair notice that a "fleeting expletive"

90. Gen. Elec. Co. v. EPA, 53 F.3d 1324, 1329 (D.C. Cir. 1995); *see also* Sec'y of Labor v. Beverly Healthcare-Hillview, 541 F.3d 193, 202 (3d Cir. 2008) (noting that the Third Circuit has endorsed the "ascertainable certainty" fair notice standard); Georgia Pac. Corp. v. Occupational Safety & Health Review Comm'n, 25 F.3d 999, 1005 (11th Cir. 1994) (applying the "ascertainable certainty" standard to interpretation of workplace safety regulation); Diamond Roofing Co., Inc. v. Occupational Safety & Health Review Comm'n, 528 F.2d 645, 649 (5th Cir. 1976) (finding that the Secretary of Labor "has the responsibility to state with ascertainable certainty what is meant by the standards he has promulgated"). Some circuit courts apply a less stringent standard than "ascertainable certainty" to agency interpretations. *See, e.g.*, Texas E. Products Pipeline Co. v. Occupational Safety & Health Review Comm'n, 827 F.2d 46, 50 (7th Cir. 1987) (holding that an agency interpretation fails to provide adequate notice only if the interpretation is "incomprehensively vague"). This Note argues, however, that the FTC's complaints and other documents can satisfy even a strict fair notice standard.

91. *See* City of Arlington v. FCC, 133 S. Ct. 1863, 1874 (2013) (noting that an agency can establish an interpretation through its adjudication or rulemaking procedures); United States v. Lachman, 387 F.3d 42, 57 (1st Cir. 2004) ("The non-public or informal understandings of agency officials concerning the meaning of a regulation are . . . not relevant" for establishing an agency's interpretation.).

92. It is not entirely clear whether courts treat the "ascertainable certainty" standard as identical to the strict standard that applies in criminal cases. One commentator has argued that "the fair notice test currently applied to civil regulations by the D.C. Circuit and the Fifth Circuit is nearly as stringent, if not as stringent, as that in criminal cases." Albert C. Lin, *Refining Fair Notice Doctrine: What Notice Is Required of Civil Regulations?*, 55 BAYLOR L. REV. 991, 1011 (2003).

or brief nudity could subject them to liability.[93] The agency's position, that such broadcasts violated a prohibition on "obscene, indecent, or profane language," contradicted earlier adjudications and policy statements without first providing notice that the agency's interpretation had changed.[94] Similarly, the D.C. Circuit found that the EPA failed to provide fair notice of its interpretation of an environmental regulation where the interpretation was never clearly stated and appeared to contradict the plain language of the regulation.[95]

In other cases, courts have found that agency interpretations satisfied the ascertainable certainty fair notice standard. Even broad agency interpretations can satisfy the standard, so long as they are sufficiently clear from past policy statements, adjudications, or other publications. In *Beverly Healthcare-Hillview*,[96] for example, the Third Circuit rejected a fair notice challenge to the Department of Labor's interpretation of a workplace health and safety standard that required employers to provide treatment "at no cost" to employees who had been exposed to a bloodborne pathogen.[97] The court found that an opinion letter and prior administrative trials had made clear that the Department of Labor interpreted "at no cost" broadly to include travel costs and compensation for time spent receiving treatment.[98] Likewise, the D.C. Circuit rejected a fair notice challenge to the Occupational Safety and Health Review Commission's interpretation of safety regulations related to "outrigger scaffolds."[99] The defendant construction company had argued that it lacked notice that its structures fell within the definition of outrigger scaffolds and therefore had to comply with certain safety requirements.[100] But the court found that the definition in the regulations, as well as a number of illustrations the agency had provided, made clear that the regulations applied to the structures at issue.[101]

93. 132 S. Ct. 2307, 2320 (2012).

94. *See id.* at 2312, 2318.

95. *See Gen. Elec. Co.*, 53 F.3d at 1331–34 (finding that there is not fair notice if the agency's "policy statements are unclear . . . the [agency's] interpretation is reasonable, and . . . the agency itself struggles to provide a definitive reading of the regulatory requirements").

96. Sec'y of Labor v. Beverly Healthcare-Hillview, 541 F.3d 193 (3d Cir. 2008).

97. *Id.* at 194.

98. *Id.* at 204–05.

99. AJP Constr., Inc. v. Sec'y of Labor, 357 F.3d 70, 76 (D.C. Cir. 2004).

100. *Id.*

101. *Id.*

Finally, it is important to distinguish the fair notice doctrine from the *Chevron* standard of deference that courts give to agency interpretations.[102] Under *Chevron*, courts must defer to an agency's interpretation of an ambiguous statute that the agency is tasked with enforcing so long as the interpretation is reasonable.[103] When the plain language of a statute does not clearly answer a particular question, "the court does not simply impose its own construction on the statute, as would be necessary in the absence of an administrative interpretation. . . . [T]he question for the court is whether the agency's answer is based on a permissible construction of the statute."[104] Thus, the *Chevron* standard gives agencies significant leeway to interpret ambiguous statutes, and courts must defer to these interpretations. The fair notice doctrine, on the other hand, requires that parties be able to ascertain with certainty what an agency's interpretation is. There is a sort of trade-off here: courts will defer to reasonable agency interpretations under *Chevron*, but agencies must make their interpretations especially clear to satisfy fair notice.

II. FTC V. WYNDHAM WORLDWIDE CORP.

Wyndham is one of the first cases to directly challenge the FTC's enforcement of data security practices under Section 5. In district court proceedings, Wyndham sought to dismiss the FTC's complaint, arguing in part that the agency had not provided fair notice of its interpretation of unfair data security practices. The district court rejected Wyndham's arguments, and the Third Circuit ultimately affirmed on interlocutory appeal.

A. FACTS OF THE CASE

Wyndham Worldwide Corporation and its subsidiaries operate hotels, sell timeshares, and license the Wyndham brand name to a number of independently owned hotels.[105] As alleged in the FTC's complaint, there were numerous flaws in Wyndham's handling of customer data and its own network infrastructure: (1) Wyndham hotels stored unencrypted credit card information; (2) management systems could be accessed with easy-to-guess passwords; (3) management systems were not protected by firewalls; (4) hotel servers could connect to the company's network without adequate

102. *See* Chevron, U.S.A., Inc. v. Natural Res. Def. Council, Inc., 467 U.S. 837, 864–66 (1984).
103. *Id.*
104. *Id.* at 843.
105. FTC v. Wyndham Worldwide Corp., 799 F.3d 236, 240 (3d Cir. 2015).

security precautions; (5) third-party vendors were granted network access without adequate restrictions; (6) reasonable measures to detect and investigate unauthorized access were not taken; and (7) Wyndham did not monitor its network for malware used in previous attacks.[106]

According to the FTC, hackers succeeded in accessing Wyndham's network on three occasions in 2008 and 2009. In April 2008, hackers gained access to the local network of a hotel in Phoenix, Arizona, and they were then able to guess the login and password for an administrator account on Wyndham's network.[107] The administrator account allowed the hackers to "obtain[] unencrypted information for over 500,000 accounts, which they sent to a domain in Russia."[108] The second attack occurred in March 2009, when malware left behind in the previous attack gave hackers access to an administrator account.[109] "[T]he hackers obtained unencrypted credit card information for approximately 50,000 customers from the management systems of 39 hotels."[110] In a third attack in late 2009, hackers again used an administrator account to obtain information for 69,000 customers from the systems of 28 hotels.[111] This series of breaches led to over $10 million of fraudulent charges on the compromised credit cards.[112]

B. PROCEDURAL HISTORY

In June 2012, the FTC filed suit in the District of Arizona, alleging that Wyndham had engaged in unfair and deceptive trade practices in violation of Section 5 of the FTC Act.[113] The case was transferred to the District of New Jersey, and Wyndham then filed a Rule 12(b)(6) motion to dismiss both the unfairness and deception claims.[114] The district court denied the motion, and it certified its decision on the unfairness claim—but not the deception claim—for interlocutory appeal. The Third Circuit granted the appeal and ultimately affirmed the district court's decision.[115] Wyndham and the FTC have now settled the case, and a consent order was filed on December 11, 2015.[116]

106. *Id.* at 240–41.
107. *Id.* at 241–42.
108. *Id.* at 242.
109. *Id.*
110. *Id.*
111. *Id.*
112. *Id.*
113. *Id.*
114. *Id.*
115. *Id.* at 240–42. Wyndham did not seek review on the deception claim.
116. *See generally* Stipulated Order for Injunction, FTC v. Wyndham Worldwide Corp., No. 12-cv-1887 (D.N.J. Dec. 11, 2015).

C. THE THIRD CIRCUIT'S ANALYSIS

The Third Circuit considered three arguments in support of Wyndham's motion: (1) that Wyndham's practices did not fall within the plain meaning of "unfair;" (2) that Congress excluded data security from the FTC's general authority by passing sector-specific data security legislation; and (3) that Wyndham lacked fair notice of the specific standards it was required to meet.

The court rejected Wyndham's contention that its alleged conduct did not meet the definition of unfair. Conduct does not need to be "unscrupulous" or "unethical" in order to be unfair.[117] And although Wyndham cited a dictionary definition of "unfair" conduct as "not equitable" or "marked by . . . deception," the court found that it would be both inequitable and deceptive to publish a privacy policy and then expose customers to "substantial financial injury" by failing to enact that policy, as Wyndham allegedly did.[118] Unfairness claims may also be brought against a business "on the basis of likely rather than actual injury," even if the business itself was the victim of a criminal act.[119] Finally, the court rejected a "*reductio ad absurdum*" argument that a broad definition of unfairness would give the FTC such expansive authority that it could "sue supermarkets that are 'sloppy about sweeping up banana peels.'"[120] If a company left out so many banana peels that it caused "619,000 customers [to] fall," the court suggested, that conduct might indeed be prohibited under Section 5.[121]

The court also held that recent legislation enacted by Congress did not exclude the FTC from regulating data security issues. Wyndham had argued that GLBA, COPPA, and FCRA granted the FTC authority within limited areas and that such grants would be redundant if the FTC could already regulate data security under Section 5.[122] The court found, however, that each piece of legislation provided for additional powers or requirements beyond those contained in Section 5.[123] FCRA, for example, "requires (rather than authorizes) the FTC to issue [certain] regulations [and] . . . expands the scope of" the Commission's enforcement authority to include

117. *Wyndham*, 799 F.3d at 244–45 (citing FTC v. R.F. Keppel & Bro., Inc., 291 U.S. 304 (1934) and FTC v. Sperry & Hutchinson Co., 405 U.S. 233, 239–40 (1972)).
118. *Id.* at 245.
119. *Id.* at 246 (internal quotation marks omitted).
120. *Id.*
121. *Id.* at 247.
122. *Id.*; *see supra* Section I.B.1 (discussing sector-specific data security statutes).
123. *Id.* at 248.

unfair and deceptive acts beyond the usual jurisdictional tests of the FTC Act.[124]

Finally, the court rejected Wyndham's argument that it had insufficient notice of the specific data security standards it was required to meet.[125] Because the FTC was merely applying a statute, rather than interpreting its own regulations or filling in statutory "gaps," a less stringent notice standard than "ascertainable certainty" applied.[126] Wyndham only needed to have fair notice of what the statute itself required to be liable. The fact that this was a civil case concerning the regulation of economic activity also supported a lower notice standard.[127] It was therefore sufficient that Wyndham could have "reasonably foresee[n]" that "a court could construe [Wyndham's] conduct as falling within the meaning of the statute."[128]

In addition, the court noted that the FTC had issued a guidebook in 2007 that described a data security plan "checklist" for companies to follow.[129] The guidebook encouraged practices like data encryption, strong passwords, and the use of firewalls that Wyndham failed to implement; the guidebook therefore could have helped Wyndham determine in advance that the FTC would view its data security measures as inadequate.[130] Furthermore, the court noted that the FTC had previously issued numerous complaints and consent orders in cases involving data security unfairness claims. These complaints could indicate the sort of conduct the FTC commissioners believed to be prohibited under Section 5.[131] In this case, the individual allegations contained in previous complaints closely resembled Wyndham's alleged practices, so Wyndham could not argue that such complaints were impermissibly vague.[132] These findings "reinforce[d] [the court's] conclusion that Wyndham's fair notice challenge fail[ed]."[133]

III. HOW TO EVALUATE FAIR NOTICE CLAIMS IN FTC DATA SECURITY ENFORCEMENT ACTIONS

This Part analyzes the Third Circuit's treatment of the fair notice issue and argues that past complaints and other guidance can satisfy the

124. *Id.*
125. *See id.* at 255.
126. *Id.* at 253–55.
127. *See id.* at 255.
128. *Id.* at 256.
129. *Id.*
130. *Id.* at 256–57.
131. *Id.* at 257–58. Consent orders, on the other hand, are "of little use . . . in trying to understand the specific requirements imposed by § 45(a)." *Id.* at 257 n.22.
132. *See id.* at 258.
133. *Id.* at 256.

"ascertainable certainty" fair notice standard in data security enforcement actions, even though the court applied a lower fair notice standard.

A. THE COURT'S TREATMENT OF THE DUE PROCESS ISSUE

The Third Circuit applied the lower fair notice standard that normally applies to economic regulation, finding that Wyndham could have had notice that the alleged data security practices were unfair based only on the statute. The court's discussion of FTC guidance suggested that the agency might satisfy the stricter ascertainable certainty standard as well.

1. The Court Suggested—but Did Not Explicitly Find—that Prior FTC Complaints Would Satisfy a Stricter Notice Standard

The Third Circuit's treatment of Wyndham's fair notice argument did not clearly address whether the FTC's past complaints, guidelines, or consent orders would have satisfied due process requirements under the stricter ascertainable certainty standard.

The court found that a lower standard applied because the FTC was merely applying the statute.[134] The relevant question was therefore "whether Wyndham had fair notice that its conduct could fall within the meaning of the statute" and not whether Wyndham had fair notice of the FTC's particular interpretation of the statute.[135] This may have been a consequence of the position Wyndham had taken during the litigation: the court emphasized that Wyndham had repeatedly asserted, in briefs and at oral argument, that the FTC had issued no rules or interpretations on data security that merited deference.[136] Wyndham therefore made the contradictory argument that the FTC had not issued any interpretations but that the notice standard for agency interpretations should apply. Because the court found that the statute itself provided notice that the alleged conduct was unfair, it did not need to reach the question of whether the FTC's had provided "ascertainable certainty" as to its interpretations on data security.[137]

---

134. *Id.* at 255.

135. *Id.*

136. *See id.* at 253 ("Wyndham's position is unmistakable: the FTC has not yet declared that cybersecurity practices can be unfair; there is no relevant FTC rule, adjudication or document that merits deference; and the FTC is asking the federal courts to interpret § 45(a) in the first instance to decide whether it prohibits the alleged conduct here.").

137. *See id.* at 255 ("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.").

After concluding that Wyndham had fair notice under the language of the statute, however, the court went on to state that the FTC's past complaints and a guidebook on data security "reinforce our conclusion that Wyndham's fair notice challenge fails."[138] This seems unnecessary to the court's holding. If the applicable standard requires only looking to the statute without reference to the agency's interpretation, then it would not matter what statements the FTC had made about unfair data security practices. The treatment of such materials was therefore ambiguous. They would seem to be irrelevant if notice depended only on the statute. At the same time, the court avoided finding explicitly that these materials would provide ascertainable certainty if they were treated as agency interpretations.

This ambiguity leaves potential uncertainty for both future enforcement actions and for businesses attempting to avoid liability. The FTC has articulated that it does intend to inform businesses through its guidelines and adjudications of what practices it considers unfair.[139] But it is unclear whether the agency can rely on such materials to target the same patterns of "unfair" conduct in the future, or if it must instead depend on judicial construction of Section 5 in new enforcement actions. Likewise, this ambiguity means it is unclear whether businesses must avoid the particular data security practices identified in past complaints, or must only avoid practices that are "unfair" as a court would construe the statute.

2. Wyndham's Due Process Claim Would Likely Fail Even Under a Stricter Fair Notice Standard

Although the Third Circuit did not explicitly find that prior complaints and publications would satisfy the ascertainable certainty standard, it easily could have. The *Wyndham* opinion includes a table comparing the allegations against the hotel chain to allegations in a previous FTC complaint against CardSystems Solutions.[140] The table demonstrates close similarities between the unfair practices alleged in each action, and the court noted that "all of the allegations in at least one of the relevant four or five

138. *See id.* at 256–58.

139. *See, e.g.*, FEDERAL TRADE COMM'N, *supra* note 2 ("The Commission's fifty data security settlements have . . . raised awareness about the risks to data . . . and the types of security failures that raise concerns."); FEDERAL TRADE COMM'N, *supra* note 76, at 1 ("There's another source of information about keeping sensitive data secure: the lessons learned from the more than 50 law enforcement actions the FTC has announced so far. These are settlements . . . [b]ut learning about alleged lapses that led to law enforcement can help your company improve its practices.").

140. *Wyndham*, 799 F.3d at 258–59 (citing Complaint, *In re* CardSystems Solutions, Inc., No. C-4168 (F.T.C. 2006), 2006 WL 2709787).

complaints [filed prior to Wyndham's alleged conduct] have close corollaries here."[141]

Comparing *Wyndham* to other cases where courts applied the ascertainable certainty standard also helps demonstrate that the standard would be satisfied here. This is not a case where the agency's interpretation contradicts a prior statement, since the FTC did not previously indicate that it considered any of Wyndham's alleged data security failures to be "fair."[142] Indeed, as the CardSystems Solutions complaint demonstrates, the FTC has consistently stated that failing to protect data using secure passwords, encryption, and firewalls may be unfair.[143] This interpretation is not at odds with the language of Section 5, either, and the FTC has repeated it in numerous complaints and guidelines.[144] The unfair data security practices that FTC complaints allege provide the kind of notice of agency interpretation that courts have upheld elsewhere: although they are not narrowly defined, they are well-illustrated by numerous examples from published guidelines and past adjudications.

As the next Section argues, courts should state clearly that FTC complaints and guidelines can provide ascertainable certainty of the agency's interpretation of unfair data security practices under Section 5. The approach in the next Section would comport with the fair notice doctrine, and would clarify the significance of FTC interpretations, without imposing an undue burden on regulated entities.

B. A FRAMEWORK FOR EVALUATING FAIR NOTICE

The following framework would provide a sensible approach to analyze fair notice issues in future FTC data security enforcement actions. It defines three categories of notice, depending on the type of interpretive guidance the FTC has provided, that fall along a scale.

At one end of the scale, the agency has provided notice through complaints and guidelines that it considers certain practices to be unfair. If a company's data security program has the same flaws the FTC has targeted

141. *Id.*

142. *Cf.* FCC v. Fox Television Stations, 132 S. Ct. 2307, 2320 (2012) (FCC failed to give fair notice to broadcasters that, contrary to prior statements, the agency's indecency policy prohibited broadcast of fleeting expletives and brief nudity).

143. *See Wyndham*, 799 F.3d at 258–59.

144. *See, e.g.*, *In re* DSW Inc., 141 F.T.C. 117, 119–20 (2006) (alleging, among other security failures, insecure passwords, unencrypted files, and a lack of firewalls); FED. TRADE COMM'N, *supra* note 78 (providing recommendations for reasonable security measures); *cf.* Gen. Elec. Co. v. EPA, 53 F.3d 1324, 1332–34 (D.C. Cir. 1995) (EPA failed to give notice of an interpretation that appeared to contradict the plain language of the regulation).

in the past, the company should know with "ascertainable certainty" that its conduct may be an unfair practice.

At the other end of the scale, the FTC's consent orders do not satisfy the fair notice standard. The security measures in these orders include more than the minimum necessary to avoid liability—they are too expansive to provide fair notice of what the FTC believes the statute requires—but companies can look to these orders for guidance on data security "best practices."

In between the two is the zone of reasonableness. Under the statute, companies have notice that they may be liable if their data security practices create risks to consumers that outweigh any benefits and cause or are likely to cause "substantial injury."[145]

1. FTC Complaints and Guidelines Provide an Interpretation that Can Satisfy the Ascertainable Certainty Standard

At one end of the spectrum, the FTC's prior complaints, guidebooks, and other statements define certain patterns of behavior as unfair. As discussed in Section III.A.2, circuit courts' analysis in other cases suggests that these materials would satisfy the ascertainable certainty standard. Companies engaging in the same patterns of conduct that the FTC has previously identified as unfair would have notice that they may be liable under Section 5.

Treating these materials as agency interpretations has several implications. The process of establishing an interpretation through enforcement allows that interpretation to evolve over time, as new complaints define conduct as unfair in response to novel technology or threats. This is particularly valuable in the context of data security, since rapid changes in technology may require new protective measures. If the FTC were required to set standards through a rulemaking process—particularly under the burdensome Magnuson-Moss procedures that apply to Section 5—any rules might become quickly outdated. Such rules might also provide little concrete guidance beyond requiring "reasonable" security, which the FTC's data security complaints and guides already emphasize.

At the same time, this leaves the agency's power constrained in important ways. Section 5(n) of the FTC Act limits unfairness enforcement to conduct that causes, or is likely to cause, "substantial injury" that outweighs any countervailing benefits and that consumers cannot avoid

145. *See* 15 U.S.C. § 45(n) (2012).

themselves.[146] This can be difficult to prove in data breach cases: for example, an administrative law judge recently dismissed the FTC's case against LabMD because the agency failed to show a likelihood of substantial consumer injury.[147] Agency interpretation would also be limited to the patterns of conduct previously alleged in complaints or described in other published guidelines. Furthermore, the *Chevron* standard allows courts to defer only to "reasonable" agency interpretations.[148] The FTC cannot interpret data security practices to be prohibited if such a reading of the statute is unreasonable. If the agency wishes to target a new data security act or practice as unfair, such an interpretation must be a reasonable reading of the statute and must be clearly announced in advance.

2. Consent Orders Provide Some Guidance but Do Not Satisfy the Ascertainable Certainty Standard

The Third Circuit in *Wyndham* found that, unlike complaints, "consent orders, which admit no liability and which focus on prospective requirements on the defendant, were of little use to it in trying to understand the specific requirements imposed by [Section 5]."[149] This is an important distinction. Commentators often group complaints and consent orders together as sources of data security guidance from the FTC.[150] The contents of each type of document differ, however, with consequences for the fair use analysis. Unlike the FTC's data security complaints, consent orders do not allege any particular conduct that violated Section 5. Nor do the orders admit any liability.[151] The requirements of such orders are also too expansive to provide clear guidance of what the FTC believes the statute requires. For example, consent orders typically require that a third-party

146. *Id.*

147. Initial Decision at 87, *In re* LabMD Inc., No. 9357 (F.T.C. Nov. 11, 2015), https://www.ftc.gov/system/files/documents/cases/151113labmd_decision.pdf [https://perma.cc/FW3G-2LST].

148. *See* Chevron, U.S.A., Inc. v. Natural Res. Def. Council, Inc., 467 U.S. 837, 864–66 (1984).

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

150. *See, e.g.*, Solove & Hartzog, *supra* note 9, at 608 (arguing that "the body of FTC settlements is the functional equivalent of privacy common law"); David Alan Zetoony, *The 10 Year Anniversary of the FTC's Data Security Program: Has the Commission Finally Gotten Too Big for Its Breaches?*, 2011 STAN. TECH. L. REV. 12, ¶¶ 8, 19 (2011) (noting that practitioners monitor both complaints and consent orders for insight into the FTC's enforcement policy); Scott, *supra* note 10, at 183 (arguing that complaints and consent orders taken together "provide limited guidance as to what a company should do (or not do) to avoid being the target of an unfairness action").

151. *See supra* Section I.B.2 (comparing the content of consent orders with that of complaints).

professional certify a company's data security program, but this is clearly not a necessary condition for companies to avoid liability under Section 5. For these reasons, consent orders cannot provide notice of an agency's interpretation that would satisfy the ascertainable certainty standard.

Nevertheless, the FTC's consent orders can provide useful guidance to companies. If a company looks to the requirements in such orders and implements a data security program that is professionally certified, with "administrative, technical, and physical safeguards appropriate to [its] size and complexity, the nature and scope of [its] activities, and the sensitivity of the personal information collected from or about consumers," this should ensure that the program is not unfair under Section 5.[152] Consent orders can thus indicate data security "best practices," even if they do not satisfy the fair notice requirement applicable to agency interpretations.

3. Companies Always Have Notice Under the Statute that They May Be Liable for Security Practices that Are Unreasonable

Where the FTC has not provided an interpretation through complaints or other guidelines that would satisfy fair notice, companies must still maintain reasonable data security. In this area, the FTC can target conduct that it has not previously identified as unfair, but courts will rely on the language of Section 5 without reference to any agency interpretation. This strikes a balance, limiting the deference the FTC receives while still allowing the agency to identify new kinds of unfair conduct in its enforcement actions.

Again, the FTC's enforcement authority is subject to the limits of Section 5(n).[153] In some cases, it may be difficult to prove that a defendant's practices were unreasonable. When the cost of a security measure is weighed against the benefit of reducing the risk of hacking, it may be hard to establish whether a company was reasonable or unreasonable in its security choices. This limitation helps protect businesses from arbitrary enforcement, especially where the agency has not provided notice that it considers a particular data security practice to be unfair.

IV. CONCLUSION

In the absence of general data security legislation or expanded rulemaking authority, the FTC is likely to continue enforcing data security

152. *See In re* Dave & Buster's, Inc., 149 F.T.C. 1449, 1455 (2010).

153. *See* 15 U.S.C. § 45(n) (2012) (providing that the FTC does not have authority to sue for violation of Section 5 "unless the act or practice causes or is likely to cause substantial injury to consumers which is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition").

as an unfair or deceptive trade practice as it has done for the past fifteen years. *Wyndham* supports this approach by affirming that the FTC's Section 5 authority does extend to data security and by rejecting the argument that the agency's enforcement efforts violated due process. Although the Third Circuit reached the correct result in the case, its fair notice analysis could have been clearer. By stating explicitly what role FTC complaints and guidelines play in establishing the agency's interpretation of unfair data security practices, and whether those materials would have satisfied a stricter fair notice standard, the court could have provided important guidance for the FTC and businesses.

The proposed framework in this Note aims to clarify the application of fair notice principles to data security enforcement. This approach has the benefit of recognizing that past complaints can provide notice of what data security practices the FTC believes to be unfair, a point on which the *Wyndham* opinion is ambiguous. It makes room for both the FTC's ability to define unfair practices and for a flexible reasonableness standard tailored to a company's particular security risks and costs. It also distinguishes between complaints, which can clearly define the FTC's interpretation, and consent orders, which may indicate best practices but do not provide notice of what the law actually requires.

The technological tools available to companies for protecting consumer data, and to hackers seeking to obtain that data, will no doubt continue to evolve rapidly. This dynamic security environment poses challenges for regulators and regulated entities alike: what is the appropriate balance between prescriptive data security rules and flexible standards, and how should those rules or standards be enforced fairly? The FTC has emphasized that a flexible reasonableness standard is the "touchstone" of its enforcement approach, but its complaints and guidelines also indicate particular patterns of conduct the Commission considers to be unfair.[154] Companies may continue to question whether the FTC gets this balance right or whether, instead, its enforcement efforts are overzealous and unpredictable. In the future, however, companies that wish to challenge FTC data security complaints resembling those the agency has previously filed are more likely to find success by arguing that their particular practices were in fact

154. *See* FED. TRADE COMM'N, *supra* note 2 (stating that "[t]he touchstone of the Commission's approach to data security is reasonableness" and that "[t]hrough its settlements, testimony, and public statements, the Commission has made clear that . . . reasonable and appropriate security is a continuous process of assessing and addressing risks . . . . The Commission has also provided educational materials to industry and the public about reasonable data security practices.").

reasonable, or that there was no substantial consumer injury, than by claiming a lack of fair notice.