NOTES

MOVING BEYOND "REASONABLE": CLARIFYING THE FTC'S USE OF ITS UNFAIRNESS AUTHORITY IN DATA SECURITY ENFORCEMENT ACTIONS

*Timothy E. Deal**

Data security breaches, which compromise private consumer information, seem to be an ever-increasing threat. To stem this tide, the Federal Trade Commission (FTC) has relied upon its authority to enforce the prohibition against unfair business practices under section 5 of the Federal Trade Commission Act ("section 5") to hold companies accountable when they fail to employ data security measures that could prevent breaches. Specifically, the FTC brings enforcement actions when it finds that companies have failed to implement "reasonable" data security measures. However, companies and scholars argue that the FTC has not provided adequate notice of which data security practices it considers "reasonable" for the purposes of section 5.

This Note explains and critically analyzes several existing proposals that seek to bring clarity to the FTC's application of its unfairness authority in the data security context and ultimately proposes a novel solution which encourages the FTC explicitly to outline its minimum data security requirements through nonlegislative rulemaking. This Note contends that the FTC should incorporate a principle of proportionality in any rule to ensure that companies know which data security measures they should implement based on the relative sensitivity of the consumer data that they retain. Additionally, this Note suggests that the FTC should incorporate a safe harbor provision so that compliant companies know that, by following the FTC's guidelines, they will be immune from section 5 enforcement actions.

* J.D. Candidate, 2017, Fordham University School of Law; B.A., 2010, Schreyer Honors College at The Pennsylvania State University. Many thanks to Professor Clare Huntington for her invaluable advice and encouragement throughout the Note-writing process. Most of all, thanks to my wife, Katie, and daughter, Marguerite, for their patience and love.

INTRODUCTION

Among the many attention-grabbing stories in the news over the summer of 2015, perhaps the most scandalous involved the Ashley Madison data security breach.[1] Targeting a site known for its focus on facilitating extramarital affairs, hackers stole users' personal information and

1. *See* Dino Grandoni, *Ashley Madison, a Dating Website, Says Hackers May Have Data on Millions*, N.Y. TIMES (July 20, 2015), http://www.nytimes.com/2015/07/21/technology/hacker-attack-reported-on-ashley-madison-a-dating-service.html?_r=0 [https://perma.cc/E9VX-VU5X].

threatened to release that information to the public unless the site was shut down.[2] The hackers ultimately followed through with their threat and released 9.7 gigabytes of private information belonging to thirty-seven million Ashley Madison users.[3]

While somewhat less sensational, another widely publicized data security breach occurred over the holiday season of 2013.[4] There, over 100 million Target shoppers' personal information, which included credit and debit card numbers, was compromised.[5] These incidents illustrate the increasing trend of high-profile data security breaches.[6]

Against this background, the Federal Trade Commission (FTC or "the Commission"), the U.S. agency tasked with enforcing consumer protection laws, has brought claims against companies that have allegedly failed to protect consumer privacy.[7] The FTC brings these claims under its authority to enforce the Federal Trade Commission Act's ("the FTC Act") section 5 ("section 5"), which prohibits "persons, partnerships, or corporations" from engaging in "unfair or deceptive acts or practices in or affecting commerce."[8]

Within this legal authority, the FTC can bring claims under *either* or *both* the "unfair" and "deceptive" prongs of section 5.[9] Early in its effort to bring the FTC Act to bear on companies that failed to protect online privacy, the FTC brought claims exclusively under its "deception

2. *See id.* Notably, that information was purported to include the users' real names and any financial transactions they made via Ashley Madison. *Id.*

3. *See* Daniel Victor, *The Ashley Madison Data Dump, Explained*, N.Y. TIMES (Aug. 19, 2015), http://www.nytimes.com/2015/08/20/technology/the-ashley-madison-data-dump-explained.html [https://perma.cc/W3NL-WD3F]. The released information included Ashley Madison users' names, addresses, and phone numbers, along with the last four digits of their credit card numbers. *Id.*

4. *See* Elizabeth A. Harris, *After Data Breach, Target Plans to Issue More Secure Chip-and-PIN Cards*, N.Y. TIMES (Apr. 29, 2014), http://www.nytimes.com/2014/04/30/business/after-data-breach-target-replaces-its-head-of-technology.html [https://perma.cc/2T7L-QM7J].

5. *Id.*

6. *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, 673 (2013) (noting that, in 2011 alone, there were "at least 855 data breaches affecting over 174 million data records . . . across the globe"). Indeed, even the U.S. government's Office of Personnel Management (OPM) suffered a major data breach in 2015, affecting over twenty-one million people. *See* Julie Hirschfeld Davis, *Hacking of Government Computers Exposed 21.5 Million People*, N.Y. TIMES (July 9, 2015), http://www.nytimes.com/2015/07/10/us/office-of-personnel-management-hackers-got-data-of-millions.html [https://perma.cc/4BFV-BRSQ]. Hackers were able to access and acquire OPM computer records, which contained an enormous amount of sensitive personal information, including Social Security numbers and fingerprints. *Id.*

7. *See* FTC v. Wyndham Worldwide Corp., 799 F.3d 236, 240 (3d Cir. 2015). The FTC also has brought general internet privacy-related actions against companies such as Google, Facebook, and Twitter. *See* Daniel J. Solove & Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, 114 COLUM. L. REV. 583, 602 (2014).

8. Federal Trade Commission Act, 15 U.S.C. § 45 (2012).

9. *See generally A Brief Overview of the Federal Trade Commission's Investigative and Law Enforcement Authority*, FED. TRADE COMM'N (July 2008) [hereinafter *Overview of FTC Authority*], https://www.ftc.gov/about-ftc/what-we-do/enforcement-authority [https://perma.cc/UH6K-A5X5].

authority."[10] However, in more recent years the FTC has increasingly relied on its "unfairness authority" as well.[11] For example, in 2012, the FTC sued Wyndham Worldwide Corporation ("Wyndham"), a global hospitality company, for violating section 5.[12] The FTC alleged that Wyndham had engaged in both "unfair" and "deceptive" practices, which facilitated three data breaches in two years.[13] Regarding Wyndham's alleged "unfair" practices, the FTC claimed that it had failed to take "reasonable" steps to prevent data breaches.[14]

Wyndham argued that the FTC lacks the authority to pursue data security claims under the unfairness prong of section 5.[15] Although the Third Circuit affirmed that the FTC does, in fact, have authority to regulate data security in this context,[16] the FTC's criteria for "fairness" remains unclear for companies because the FTC has yet to explain what practices it considers to be "reasonable."[17] As a result, there are a number of conflicting scholarly proposals promoting a data security enforcement regime that better informs companies of the FTC's minimum data security requirements.[18]

The purpose of this Note is twofold. First, this Note analyzes the merits of these scholarly proposals. Then, this Note proposes a novel solution to this issue that strives to maximize important societal goals: (1) the need for better notice to regulated entities;[19] (2) the FTC's goal of robust consumer protection;[20] and (3) the FTC's need for administrative flexibility given the dynamic technological environment it regulates.[21]

Accordingly, Part I of this Note explores the development of the FTC's section 5 authority. Next, Part II addresses the application of the FTC's section 5 authority in the online privacy and data security context. Part III

---

10. *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, 131 (2008); *see also infra* Part II.A.

11. *See* Scott, *supra* note 10, at 134.

12. *See* Press Release, Fed. Trade Comm'n, FTC Files Complaint Against Wyndham Hotels for Failure to Protect Consumers' Personal Information (June 26, 2012), https://www.ftc.gov/news-events/press-releases/2012/06/ftc-files-complaint-against-wyndham-hotels-failure-protect [https://perma.cc/R4X8-PJ6G].

13. *See* FTC v. Wyndham Worldwide Corp., 799 F.3d 236, 240 (3d Cir. 2015).

14. *See id.* at 241.

15. *See id.* at 240.

16. *See id.* at 259.

17. In *Wyndham*, the Third Circuit held that the FTC provided *constitutionally* adequate fair notice regarding its criteria for fair data security practices. *See id.* That does not mean, however, that the FTC *actually* has provided adequate notice. *See, e.g.*, Stegmaier & Bartnick, *supra* note 6, at 706–07 ("Even if the FTC is deemed to have provided legally required fair notice of required data-security practices under [s]ection 5, the FTC's policy has not likely been effectively communicated.").

18. *See* discussion *infra* Part III.A.

19. *See, e.g.*, Stegmaier & Bartnick, *supra* note 6, at 706.

20. *What We Do*, FED. TRADE COMM'N, https://www.ftc.gov/about-ftc/what-we-do (last visited Mar. 27, 2016) [https://perma.cc/EX3M-8H93].

21. *See* Andrew Serwin, *The Federal Trade Commission and Privacy: Defining Enforcement and Encouraging the Adoption of Best Practices*, 48 SAN DIEGO L. REV. 809, 852 (2011).

lays out and assesses several scholarly proposals regarding how the FTC can better provide regulated companies with proper notice of what it considers to be "reasonable" data security requirements under its unfairness authority. Finally, Part IV proposes a resolution that is geared toward balancing adequate notice to companies, consumer protection, and administrative flexibility.

I. THE FTC AND ITS AUTHORITY UNDER SECTION 5: AN OVERVIEW

Today, various companies and other entities store a vast amount of personal information electronically.[22] According to the Government Accountability Office (GAO), data security breaches occur where there is an "unauthorized or unintentional exposure, disclosure, or loss of sensitive personal information."[23] A variety of methods can facilitate a data security breach, such as theft or loss of equipment, hacking, unintentional disclosure of personal information, and use of other inadequate data security practices.[24] The FTC has identified many inadequate data security practices including lack of encryption, failure to implement customary security practices, and the use of weak passwords.[25] No matter the cause, data security breaches can compromise individuals' personally identifiable information[26] (PII).

Although information regarding the consequences of data security breaches is limited,[27] it is beyond question that they can lead to identity theft,[28] which constitutes a range of criminal activities and individual injuries.[29] Criminal activities include the unauthorized use of credit cards or the opening of a fraudulent bank account.[30] These crimes can result in anything from the inconvenience of having to cancel a credit card to substantial financial loss.[31]

To stem the tide of increasing data security breaches, the FTC has stepped in to hold companies accountable where such breaches are

22. *See* U.S. GOV'T ACCOUNTABILITY OFFICE, GAO-07-737, DATA BREACHES ARE FREQUENT, BUT EVIDENCE OF RESULTING IDENTITY THEFT IS LIMITED; HOWEVER, THE FULL EXTENT IS UNKNOWN 1 (2007) ("[M]any different sectors and entities now maintain electronic records containing vast amounts of personal information on virtually all American consumers.").

23. *See id.* at 2.

24. *See* Scott, *supra* note 10, at 144–45.

25. *See* Solove & Hartzog, *supra* note 7, at 651–55 (listing twenty-six inadequate data security practices gleaned from FTC complaints).

26. *See* U.S. GOV'T ACCOUNTABILITY OFFICE, *supra* note 22, at 2. The GAO has defined PII as "any information that can be used to distinguish or trace an individual's identity . . . such as name, Social Security Number, driver's license number, and mother's maiden name." *See id.* at 2 n.2.

27. *See id.* at 21.

28. *See id.*

29. *See id.* at 2.

30. *See id.*

31. *See id.*

avoidable.[32] More specifically, where companies have failed to take "reasonable" steps to prevent data breaches and protect consumer data, the FTC has brought cases using its statutory authority under section 5 of the FTC Act.[33]

To establish relevant background, Part I.A provides a brief introduction of the FTC's general authority under section 5. Then, Part I.B summarizes the development of that authority.

A. An Overview of the FTC's Authority Under Section 5

The FTC is the federal agency tasked with protecting consumers and promoting competition.[34] When it was initially created in 1914, Congress gave the FTC the power to enforce section 5 of the FTC Act, which included a prohibition against "unfair methods of competition in commerce."[35] Accordingly, for the first two decades of its existence, the FTC's authority was limited to regulating antitrust issues.[36]

In 1938, Congress amended section 5 to include "unfair or deceptive acts or practices in commerce."[37] As stated by the U.S. Supreme Court,

> The amendment added the phrase "unfair or deceptive acts or practices" to the section's original ban on "unfair methods of competition" and thus made it clear that Congress, through [section] 5, charged the FTC with protecting consumers as well as competitors. The House Report on the amendment summarized congressional thinking: "[T]his amendment makes the consumer, who may be injured by an unfair trade practice, of equal concern, before the law, with the merchant or manufacturer injured by the unfair methods of a dishonest competitor."[38]

Thus, Congress has granted authority to the FTC to enforce the prohibition against unfair or deceptive practices to better protect consumers.[39]

Congress also has granted the FTC enforcement authority under other statutes, such as the Fair Credit Reporting Act,[40] the Gramm-Leach-Bliley Act,[41] and the Children's Online Privacy Protection Act.[42] However,

---

32. *See* Solove & Hartzog, *supra* note 7, at 588.

33. *See* Federal Trade Commission Act, 15 U.S.C. § 45 (2012).

34. *See id.*; *What We Do*, *supra* note 20.

35. Federal Trade Commission Act of 1914, Pub. L. No. 63-203, § 5, 38 Stat. 717, 719 (codified as amended at 15 U.S.C. § 45(a)).

36. *See* Serwin, *supra* note 21, at 814–15.

37. Pub. L. No. 75-447, § 5, 52 Stat. 111, 111 (1938) (codified as amended at 15 U.S.C. § 45(a)).

38. FTC v. Sperry & Hutchinson Co., 405 U.S. 233, 244 (1972) (quoting H.R. REP. NO. 75-1613, at 3 (1937)). The organizational structure of the FTC reflects its evolving purpose as a joint antitrust and consumer protection agency, as two of its primary departments are the Bureau of Competition and the Bureau of Consumer Protection. *See Bureaus & Offices*, FED. TRADE COMM'N, https://www.ftc.gov/about-ftc/bureaus-offices (last visited Mar. 27, 2016) [https://perma.cc/NLY6-3SAH].

39. *See* Serwin, *supra* note 21, at 814–15.

40. Fair Credit Reporting Act, Pub. L. No. 91-508, § 601, 84 Stat. 1114 (1970) (codified as amended in scattered sections of 15 U.S.C.).

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

discussion of the FTC's enforcement authority under these statutes is beyond the scope of this Note.

B. Development of the FTC's Authority Under Section 5

Since the enactment of section 5, the FTC has sought to flesh out the contours of its authority under the deception and unfairness prongs of section 5.[43] Part I.B.1 provides a brief overview of the development of the FTC's deception authority, and Part I.B.2 discusses the development of the FTC's unfairness authority. Part I.B.3 describes the FTC's administrative authority under section 5. Lastly, Part I.B.4 explains the choice that the FTC has between adjudication and judicial enforcement when seeking to hold companies accountable under section 5.

1. Deception Authority

Section 5 gives the FTC the authority to enforce Congress's prohibition against deceptive business practices.[44] However, as Congress did not define "deceptive practices" in section 5, the FTC had to develop its own definition over time.[45]

In 1983, the FTC issued a policy statement identifying those elements that it deemed relevant in considering whether a given act or practice was deceptive.[46] The FTC noted that it would consider a given action deceptive "if there is a representation, omission or practice that is likely to mislead the consumer acting reasonably in the circumstances, to the consumer's detriment."[47] Therefore, to show that a defendant has acted with "deception" in violation of section 5, the FTC must prove three elements: (1) there was a material representation, omission, or practice; (2) the representation, omission, or practice was likely to mislead consumers; and (3) the consumers were acting reasonably under the circumstances.[48]

---

42. Children's Online Privacy Protection Act of 1998, Pub. L. No. 105-277, 112 Stat. 2681 (codified as amended at 15 U.S.C. §§ 6501–6506).

43. *See* Serwin, *supra* note 21, at 821–23.

44. *See* 15 U.S.C. § 45(a)(1) (2012).

45. *See* Serwin, *supra* note 21, at 821–23.

46. *See* Cliffdale Assocs., Inc., 103 F.T.C. 110, 174–84 (1984) (appending Letter from James C. Miller III, Chairman, Fed. Trade Comm'n, to Hon. John D. Dingell, Chairman, Comm. on Energy & Commerce, U.S. House of Representatives (Oct. 14, 1983)).

47. *See id.* at 176.

48. *See, e.g.*, FTC v. Verity Int'l, Ltd., 124 F. Supp. 2d 193, 200 (S.D.N.Y. 2000) (laying out the established factors that the FTC must show to establish liability under its deception authority). In the context of online privacy, the FTC initially relied on the deception prong of its section 5 authority to hold companies accountable for failing to deliver on the data security promises laid out in their privacy policies. *See* discussion *infra* Part II.A. Although the FTC's deception authority plays an important role in its data security jurisprudence, further discussion is beyond the scope of this Note.

2. Unfairness Authority

Section 5 also gives the FTC the authority to enforce the prohibition against unfair business practices.[49] Following the amendment that added the prohibition against "unfair and deceptive practices" to section 5,[50] the FTC spent several decades developing the meaning of "unfair" practices.[51] Over that time, the Supreme Court held that "unfair" practices do not need to be enumerated or set in stone and that the concept can be defined fluidly over time.[52]

In response to a request from the Senate Committee on Commerce, Science, and Transportation, the FTC issued a policy statement in 1980 setting forth its interpretation of "unfair practices."[53] Specifically, the FTC explained that an unfairness determination requires consideration of three factors: "(1) whether the practice injures consumers; (2) whether it violates established public policy; [and] (3) whether it is unethical or unscrupulous."[54]

Despite the enumeration of these three factors, unfairness determinations eventually relied primarily upon the policy statement's "consumer injury" prong.[55] According to the policy statement, when analyzing this prong, the FTC was required to find that consumer injury satisfied three tests: "[(1)] [i]t must be substantial; [(2)] it must not be outweighed by any countervailing benefits to consumers or competition that the practice produces; and [(3)] it must be an injury that consumers themselves could not reasonably have avoided."[56] Congress subsequently codified these tests under section 5.[57]

---

49. *See* 15 U.S.C. § 45(a)(1).

50. *See supra* note 37 and accompanying text.

51. The FTC primarily interpreted the meaning of unfair practices by means of agency adjudication. *See* FTC v. Wyndham Worldwide Corp., 799 F.3d 236, 240 (3d Cir. 2015). This practice was permissible under Supreme Court case law holding that federal agencies have the discretion to promulgate policy via either rulemaking or adjudication. *See* SEC v. Chenery Corp., 332 U.S. 194, 202–03 (1947).

52. *See* FTC v. Raladam Co., 283 U.S. 643, 648 (1931) (discussing "unfairness" in the context of competition); *see also* FTC v. Sperry & Hutchinson Co., 405 U.S. 233, 239–40 (1972) (concluding that, under section 5, the FTC has the authority to proscribe unfair practices vis-à-vis consumers).

53. *See* Letter from the Fed. Trade Comm'n to Hon. Wendell Ford and Hon. John Danforth, Senate Comm. on Commerce, Sci. & Transp. (Dec. 17, 1980), *appended to* Int'l Harvester Co., 104 F.T.C. 949, 1070–72 (1984) [hereinafter FTC Policy Statement on Unfairness]; *cf. supra* notes 46–47 and accompanying text (discussing the use of a policy statement to clarify the FTC's deception authority).

54. FTC Policy Statement on Unfairness, *supra* note 53, at 1072.

55. *See* Serwin, *supra* note 21, at 832.

56. FTC Policy Statement on Unfairness, *supra* note 53, at 1073.

57. *See* 15 U.S.C. § 45(n) (2012); *see also* FTC v. Wyndham Worldwide Corp., 799 F.3d 236, 244 (3d Cir. 2015) (outlining the development of the FTC's unfairness authority and citing the three-part test required for a finding of unfairness under section 5).

3. Administrative Authority Under Section 5

In addition to granting substantive enforcement authority under section 5,[58] Congress also has given the FTC rulemaking authority.[59] Specifically, Congress has empowered the FTC to promulgate "interpretive rules and general statements of policy with respect to unfair or deceptive practices"[60] and "rules which define with specificity acts or practices which are unfair or deceptive acts or practices."[61] These two statutory grants of rulemaking authority demonstrate the distinction between nonlegislative and legislative rules.[62]

Legislative rules are rules that an agency promulgates pursuant to congressionally delegated authority that an agency intends to have the binding force of law.[63] To justify this binding effect, agencies must issue these rules by following strict procedures set forth in the Administrative Procedure Act[64] (APA), such as providing for a public notice and comment period and publishing a proposed rule in the Federal Register.[65]

With respect to the FTC's legislative rulemaking authority under section 5, it is also required to "provide an opportunity for an informal hearing."[66] As this and other requisite procedures for the section 5 rulemaking process make it rather arduous,[67] the FTC has tended to promulgate policy through adjudication.[68]

Where rules do not follow the strict procedural requirements for legislative rules or are not promulgated pursuant to specific statutory

---

58. *See supra* Part I.B.1–2 (discussing the FTC's authority to enforce Congress's prohibition against deceptive and unfair business practices).

59. *See* 15 U.S.C. § 57a. Below, this Note proposes that the FTC should use its nonlegislative rulemaking authority under section 5 to define "unfair practices" in the data security context. *See infra* Part IV.A.

60. 15 U.S.C. § 57a(a)(1)(A).

61. *Id.* § 57a(a)(1)(B).

62. *See* Robert A. Anthony, *Interpretive Rules, Policy Statements, Guidances, Manuals, and the Like—Should Federal Agencies Use Them to Bind the Public?*, 41 DUKE L.J. 1311, 1321–23 (1992) (describing the distinction between nonlegislative and legislative rules).

63. *See id.* at 1322.

64. *See* 5 U.S.C. §§ 551–559 (2012).

65. *See id.* § 553(b).

66. 15 U.S.C. § 57a(b)(1)(C). The FTC also is required to "publish notice of proposed rulemaking" and "allow interested persons to submit written data, views, and arguments." *Id.* § 57a(b)(1)(A)–(B). Additionally, to promulgate a rule, the FTC must find that the "unfair or deceptive acts or practices which are the subject of the proposed rulemaking are prevalent." *Id.* § 57a(b)(3). Lastly, the FTC is required to follow procedures set out in 5 U.S.C. § 553, which sets out the procedural requirements for informal rulemaking. 15 U.S.C. § 57a(b)(1). These procedures include requiring an agency to publish a rule in the Federal Register and to allow for a public comment period. *See* 5 U.S.C. § 553(b).

67. *See* Stegmaier & Bartnick, *supra* note 6, at 692.

68. *See Prepared Statement of the Fed. Trade Comm'n on Data Security: Before the Subcomm. on Commerce, Mfg. & Trade of the H. Comm. on Energy & Commerce*, 112th Cong. 11 (2011) (statement of Edith Ramirez, Comm'r, Fed. Trade Comm'n) ("[E]ffective consumer protection requires that the Commission be able to promulgate these rules in a more timely and efficient manner."). As noted above, federal agencies have the discretion to promulgate policy through either adjudication or rulemaking. *See supra* note 51.

authority, they are termed "nonlegislative."[69] Although they can take on many different forms, interpretive rules and policy statements are two paradigmatic examples of nonlegislative rules.[70] An interpretive rule is an agency statement that explains to the public the agency's interpretation of the statutes and rules that it administers.[71] By contrast, when an agency issues policy statements, it is seeking to notify the public of the manner in which it intends to exercise its discretionary power in the future.[72] While nonlegislative rules afford agencies more flexibility in communicating policy to the public, they also tend to receive less deferential treatment in court.[73]

4. Enforcement: The Choice Between Adjudication and Judicial Action

When bringing an action enforcing section 5, the FTC can opt to pursue either an administrative adjudication[74] or judicial enforcement.[75] If it chooses the administrative process, the FTC issues a complaint against a defendant,[76] who then has the option to settle with the FTC by signing a consent decree.[77] Signing a consent decree is not an admission of liability.[78] Alternatively, the defendant can choose to contest the FTC's allegations, in which case there will be a hearing before an Administrative Law Judge[79] (ALJ). Either party can appeal the ALJ's decision to the Commission itself.[80] A defendant can appeal the Commission's final decision to the relevant federal court of appeals.[81]

Rather than taking the administrative route when enforcing section 5, the FTC also can file a complaint in federal court seeking such remedies as temporary restraining orders, preliminary injunctions, or consumer

---

69. *See* Anthony, *supra* note 62, at 1322–23.

70. *See id.* at 1323.

71. *See* Am. Mining Cong. v. Mine Safety & Health Admin., 995 F.2d 1106, 1109 (D.C. Cir. 1993).

72. *See id.* For examples of policy statements, see *supra* notes 46, 53.

73. *See* United States v. Mead Corp., 533 U.S. 218, 226–27 (2001) (holding that nonlegislative rules such as interpretive rules and policy statements are not necessarily entitled to significant deference from courts where there is no indication that Congress meant for the rule to carry the force of law); *see also infra* Part IV.B.

74. *See* 15 U.S.C. § 45(b) (2012).

75. *See id.* § 53(a)–(b).

76. *See* 16 C.F.R. § 3.11(a) (2015).

77. *See id.* § 2.31; *see also Overview of FTC Authority*, *supra* note 9, at II.A.1.a.

78. *See* 16 C.F.R. § 2.32 ("[A consent decree] may state that the signing thereof is for settlement purposes only and does not constitute an admission by any party that the law has been violated as alleged in the complaint."). Accordingly, defendants are incentivized to settle with the FTC as soon as possible, which, in the data security context, has led to a lack of judicial or administrative determinations to provide guidance to companies regarding what the FTC deems as "unfair" data security practices. *See* Solove & Hartzog, *supra* note 7, at 588; *infra* note 150.

79. *See* 16 C.F.R. § 3.1.

80. *See id.* § 3.52(b)(1). The Commission generally consists of five presidentially nominated commissioners. *See Commissioners*, FED. TRADE COMM'N, https://www.ftc.gov/about-ftc/commissioners (last visited Mar. 27, 2016) [https://perma.cc/QHT8-8DKX].

81. *See* 15 U.S.C. § 45(c) (2012).

redress.[82] Indeed, even when enforcing administrative decisions, the FTC requires the aid of a court.[83]

Judicial enforcement has the advantage of enabling the FTC to pursue injunctive and monetary relief at the same time.[84] However, administrative adjudication provides certain procedural advantages such as giving the FTC the first opportunity to make findings of fact[85] and keeping the first appellate step within the Commission.[86] Moreover, if an administrative decision goes up for judicial review, a reviewing court will likely afford it significant deference where it involves an FTC interpretation of a statute.[87] Given these procedural advantages, the FTC typically opts for the administrative process, particularly when faced with unique, fact-driven cases.[88]

Having examined the FTC's authority under section 5 generally, this Note now considers the application of that authority to online privacy and data security.

II. JUST BE REASONABLE!: THE APPLICATION OF THE FTC'S UNFAIRNESS AUTHORITY IN THE DATA SECURITY CONTEXT

Over the past decade and a half, the FTC has been on the forefront of online privacy enforcement.[89] In that capacity, the Commission has brought the section 5 authority discussed in Part I to bear in a new and evolving context. Accordingly, Part II.A explains the development of the FTC's general internet privacy enforcement. Part II.B discusses how the FTC has applied its unfairness authority in the data security context. Finally, Part II.C considers recent challenges to the FTC's use of its unfairness authority in the data security context.

A. Evolution of the FTC's Online Privacy Enforcement

In the early days of the internet, the FTC addressed online privacy concerns by encouraging industry self-regulation.[90] The rationale at the time was that the free market would punish any companies that failed to

82. *See id.* § 53(a)–(b).

83. *See Overview of FTC Authority*, *supra* note 9, at II.A.2 (noting that the FTC must receive the aid of a court to obtain consumer redress for violations of administrative orders).

84. *See id.*

85. *See id.*

86. *See* 16 C.F.R. § 3.52(b)(1) (2015); *supra* note 80 and accompanying text.

87. *See generally* Chevron, U.S.A., Inc. v. Nat. Res. Def. Council, 467 U.S. 837 (1984) (holding that, in certain circumstances, courts should afford significant deference to an agency's interpretation of a statute).

88. *See Overview of FTC Authority*, *supra* note 9, at II.A.2. Thus, in the data security context, the FTC has primarily proceeded via the administrative process. *See* Stegmaier & Bartnick, *supra* note 6, at 690.

89. *See* FTC v. Wyndham Worldwide Corp., 799 F.3d 236, 240 (3d Cir. 2015); Stegmaier & Bartnick, *supra* note 6, at 674.

90. *See* FED. TRADE COMM'N, PRIVACY ONLINE: A REPORT TO CONGRESS 2 (1998), https://www.ftc.gov/sites/default/files/documents/reports/privacy-online-report-congress/priv-23a.pdf [https://perma.cc/A77W-AZ2F]; *see also* Scott, *supra* note 10, at 130.

protect consumer data.[91] Thus, the FTC limited its section 5 enforcement in the internet privacy context to situations where a company failed to live up to the promises it had made in its published privacy policy.[92]

This enforcement strategy reflected what is called the "notice-and-choice model" of privacy enforcement.[93] This model sought to encourage companies to develop detailed privacy policies so that consumers would be informed as to how companies would use their personal information.[94]

As applied in FTC enforcement actions, the notice-and-choice model corresponds with the FTC's deception authority under section 5.[95] For example, in its first internet privacy enforcement action, the FTC alleged that GeoCities, a website that enabled users to organize personal, interest-based websites in topical "neighborhoods," had misrepresented its actual information collection practices in its published privacy policy.[96] The FTC's complaint resulted in a consent order wherein GeoCities agreed to implement better privacy practices.[97] The FTC continued to use this enforcement strategy for several years.[98]

Despite its success in early, internet-based section 5 enforcement actions,[99] the FTC determined that industry self-regulation and its enforcement of privacy policies were insufficient to ensure the protection of consumer information online and decided to engage in more robust enforcement.[100] As a result, the FTC began relying more heavily on its

91. *See* Scott, *supra* note 10, at 130.

92. *See id.*

93. *See* Serwin, *supra* note 21, at 815–16. The model finds its origins in a collection of widely accepted principles, which reflect best practices in privacy protection known as the Fair Information Practice Principles. *See generally* FED. TRADE COMM'N, *supra* note 90, at 7–11. The Fair Information Practice Principles consist of "(1) Notice/Awareness; (2) Choice/Consent; (3) Access/Participation; (4) Integrity/Security; and (5) Enforcement/Redress." *Id.* at 7.

94. *See* FED. TRADE COMM'N, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE: RECOMMENDATIONS FOR BUSINESSES AND POLICYMAKERS 2 (2012), https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf [https://perma.cc/YJD5-879Y]. Notably, the notice-and-choice model has been criticized for incentivizing companies to create very long privacy policies that are hardly understandable to most consumers. *See id.*; *see also infra* notes 210–12 and accompanying text.

95. *See* Serwin, *supra* note 21, at 812 (arguing that the notice-and-choice model corresponds with the FTC's section 5 deception authority).

96. *See* GeoCities, 127 F.T.C. 94, 96–98 (1999) (laying out the FTC's allegations of deception); *see also* Press Release, Fed. Trade Comm'n, Internet Site Agrees to Settle FTC Charges of Deceptively Collecting Personal Information in Agency's First Internet Privacy Case (Aug. 13, 1998) [hereinafter GeoCities Press Release], https://www.ftc.gov/news-events/press-releases/1998/08/internet-site-agrees-settle-ftc-charges-deceptively-collecting [https://perma.cc/S8WM-24E4].

97. *See GeoCities*, 127 F.T.C. at 121–33; *see also* GeoCities Press Release, *supra* note 96 ("GeoCities has agreed to post on its site a clear and prominent Privacy Notice, telling consumers what information is being collected and for what purpose, to whom it will be disclosed, and how consumers can access and remove the information.").

98. *See* Serwin, *supra* note 21, at 835.

99. *See* discussion *supra* notes 96–98 and accompanying text.

100. *See* Scott, *supra* note 10, at 130–31.

unfairness authority.[101] This adjustment in enforcement strategy signaled a new focus on the "harm-based model" of privacy enforcement,[102] which seeks to protect consumers from specific harms such as economic loss and unauthorized intrusion into their private lives.[103]

The FTC first exercised its unfairness authority in the online privacy context in an enforcement action against ReverseAuction.com.[104] There, the FTC alleged that ReverseAuction.com, an early eBay competitor, had signed into eBay, obtained eBay users' personal information, and then sent those users unsolicited emails misrepresenting that their eBay accounts were going to expire.[105] The FTC argued that the company's deeds were actionable under section 5 as either a deceptive or unfair business practice.[106] With regard to unfairness, the FTC, relying on the three-part test required for a finding of unfairness under section 5,[107] alleged that ReverseAuction.com's business practices were "likely to cause substantial injury to consumers which [was] not reasonably avoidable by consumers and not outweighed by countervailing benefits to consumers or competition, and therefore was . . . an unfair practice."[108]

Although the FTC commissioners approved the resulting consent order, the FTC's reliance on its unfairness authority elicited several dissenting opinions.[109] FTC Commissioners Thomas Leary and Orson Swindle argued that the use of the FTC's unfairness authority was inappropriate because they did not believe the consumer injury was sufficiently substantial.[110] Conversely, FTC Commissioner Mozelle Thompson argued that the use of the FTC's unfairness authority was appropriate because the consumers had indeed suffered a significant injury as their individual "privacy expectation[s]" and "consumer confidence" generally were undermined.[111] As demonstrated by the FTC's increasing use of its unfairness authority in

101. *See id.* at 143.

102. *See* Serwin, *supra* note 21, at 815–16.

103. *See* FED. TRADE COMM'N, *supra* note 94, at 2. Like the notice-and-choice model, the harm-based model has faced criticism. *See id.* ("[The harm-based model has] been criticized for failing to recognize a wider range of privacy-related concerns, including reputational harm or the fear of being monitored."); *see also infra* notes 211–12. In contrast to the notice-and-choice model, which corresponds to the FTC's deception authority, *see supra* note 95 and accompanying text, the harm-based model corresponds to the FTC's unfairness authority. *See* Serwin, *supra* note 21, at 812.

104. *See* Serwin, *supra* note 21, at 835–36.

105. *See* Complaint ¶¶ 6–13, FTC v. Reverseauction.com, No. 1:00-CV-00032 (D.D.C. Jan. 6, 2000), https://www.ftc.gov/sites/default/files/documents/cases/2000/01/www.ftc_.gov-reversecmp.htm [https://perma.cc/RF6G-437L]; *see also* Press Release, Fed. Trade Comm'n, Online Auction Site Settles FTC Privacy Charges (Jan. 6, 2000) [hereinafter ReverseAuction.com Press Release], https://www.ftc.gov/news-events/press-releases/2000/01/online-auction-site-settles-ftc-privacy-charges [https://perma.cc/KS4M-KD7C].

106. Complaint, *supra* note 105, ¶¶ 16–17.

107. *See supra* notes 56–57 and accompanying text.

108. Complaint, *supra* note 105, ¶ 17.

109. *See* ReverseAuction.com Press Release, *supra* note 105; *see also* Serwin, *supra* note 21, at 836–37.

110. *See* ReverseAuction.com Press Release, *supra* note 105.

111. *See id.*

online privacy and data security-related enforcement actions,[112] Commissioner Thompson's view won the day.[113]

B. Increasing Use of the FTC's Unfairness Authority in the Data Security Context

In addition to applying its unfairness authority to online privacy generally,[114] the FTC also applies this authority in actions against companies that have suffered data security breaches.[115] As noted above,[116] when the FTC brings actions pursuant to its unfairness authority under section 5, it must show that the defendant-company was engaged in an act or practice that "cause[d] or [was] likely to cause substantial injury to consumers which [was] not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers."[117]

In the data security context, the FTC primarily seeks to hold companies accountable via administrative action,[118] and its complaints frequently allege that defendants engaged in "unfair" practices by failing to employ "reasonable" or "adequate" data security measures to protect consumer data.[119] As a result of the FTC's administrative process, the FTC and a defendant-company almost always enter into a consent order wherein the defendant agrees to implement improved security practices and submit to data security-related oversight for a period of up to twenty years.[120]

For example, in *BJ's Wholesale Club, Inc.*,[121] the FTC alleged that hackers accessed unencrypted consumer data such as bank and credit card information as a result of BJ's Wholesale Club's ("BJ's") inadequate data security practices.[122] The FTC argued that BJ's had failed to use "reasonable and appropriate" data security measures to protect consumer information.[123] This failure, according to the complaint, was sufficient to enable the FTC to bring an enforcement action against BJ's relying solely upon its unfairness authority.[124] Rather than contesting the FTC's allegations, BJ's immediately entered into a consent agreement with the

112. *See infra* Part II.B.
113. *See* Serwin, *supra* note 21, at 837.
114. *See* discussion *supra* notes 104–13 and accompanying text.
115. *See* Scott, *supra* note 10, at 143.
116. *See supra* Part I.B.2.
117. 15 U.S.C. § 45(n) (2012); *see also supra* Part I.B.2.
118. *See* 15 U.S.C. § 45(b). For a description of this process, see *supra* notes 77–81 and accompanying text.
119. *See* Stegmaier & Bartnick, *supra* note 6, at 692–93. The principal argument against the FTC's strategy in the data security context is that it does not specify which practices are "reasonable" or "adequate." *See infra* Part III.A.2–3.
120. *See* Stegmaier & Bartnick, *supra* note 6, at 690–91.
121. 140 F.T.C. 465 (2005).
122. *See id.* at 466–68.
123. *See id.* at 467. In particular, the complaint alleged that "[a]mong other things," BJ's had failed to encrypt sensitive consumer information, stored information in such a way that it could be accessed easily and anonymously, and failed to use "readily available security measures" to identify unauthorized access to consumer data. *Id.*
124. *See id.* at 468.

FTC in which it agreed, among other things, to implement more robust data security procedures and submit to biennial third-party data security auditing.[125] Other FTC data security cases relying on the FTC's unfairness authority generally follow a similar pattern.[126] Consequently, companies and scholars argue that there is a significant lack of case law or adjudicatory guidance regarding what minimum data security measures the FTC requires of companies under its unfairness authority.[127]

C. Challenges to the Use of the FTC's Unfairness Authority in the Data Security Context

In response to the FTC's use of its unfairness authority in the data security context, respondents' primary challenge is that the Commission's complaints only vaguely terms defendants' "unfair" practices as "unreasonable" or "inadequate."[128] Thus, companies contend that they have not been given sufficient notice as to the FTC's data security requirements.[129] Two recent examples that illustrate this challenge are *LabMD, Inc.*[130] and *FTC v. Wyndham Worldwide Corp.*[131]

In *LabMD*, the FTC filed an administrative complaint against LabMD, a company that tests medical samples and reports test results to consumers' healthcare providers.[132] By means of its testing procedures, LabMD acquires personal consumer data such as names, Social Security numbers, and medical information.[133] Additionally, the company uses computers to transmit information including private consumer data.[134] The FTC alleged that LabMD "failed to provide reasonable and appropriate security for personal information" by, "[a]mong other things," not having a comprehensive information security plan, not implementing commonly used security measures, and not training its employees in effective data security practices.[135] The FTC contended that, as a result of these inadequacies, an identify thief in California was found in possession of consumer data, such as names and Social Security numbers, illegally obtained from LabMD.[136]

---

125. *See id.* at 469–73.

126. *See, e.g.*, Dave & Buster's, Inc., 149 F.T.C. 1449 (2010); DSW Inc., 141 F.T.C. 117 (2006).

127. *See* Solove & Hartzog, *supra* note 7, at 588; *see also infra* Parts II.C, III.A.

128. *See, e.g.*, Stegmaier & Bartnick, *supra* note 6, at 692–93 (noting that, in the data security context, the FTC has "use[d] terms like 'reasonable,' 'appropriate,' 'adequate,' or 'proper'" when outlining which practices a defendant-company has failed to use and that these "failures 'taken together' violate [s]ection 5").

129. *See, e.g.*, FTC v. Wyndham Worldwide Corp., 799 F.3d 236, 240 (3d Cir. 2015).

130. No. 9357 (F.T.C. Feb. 5, 2016), https://www.ftc.gov/enforcement/cases-proceedings/102-3099/labmd-inc-matter [https://perma.cc/3PP7-PN4N].

131. 799 F.3d 236 (3d Cir. 2015).

132. Complaint at 1, LabMD, Inc., No. 9357 (F.T.C. Feb. 5, 2016), https://www.ftc.gov/sites/default/files/documents/cases/2013/08/130829labmdpart3.pdf [https://perma.cc/7LDS-8LLQ].

133. *See id.* at 2.

134. *See id.*

135. *See id.* at 3.

136. *See id.* at 5.

Rather than capitulating to the FTC's complaint,[137] LabMD filed an answer in which it argued that the FTC had failed to give adequate notice as to "what data-security practices the Commission believes [s]ection 5 . . . forbids or requires."[138] In so doing, it became one of the few companies to challenge the FTC's use of its unfairness authority in the data security context.[139]

Wyndham represents another case in which a company responded to an alleged violation of section 5 for failing to implement "reasonable" data security practices by arguing that the FTC had not provided adequate notice as to what its minimum data security requirements are.[140] There, the FTC alleged that Wyndham, a global hospitality company, engaged in data security practices that, "taken together, unreasonably . . . exposed consumers' personal data to unauthorized access and theft."[141] These inadequate practices included, for example, the storage of credit card information as easily readable text, the failure to use firewalls to secure sensitive information, and the failure to use "reasonable measures to detect and prevent unauthorized access."[142] The FTC alleged that Wyndham's "unreasonable" data security practices led to three data security breaches in a two-year period, each perpetrated by hackers.[143]

On interlocutory appeal before the Third Circuit from the district court's denial of its motion to dismiss, Wyndham argued that the FTC had not provided constitutionally adequate fair notice that its practices could violate section 5.[144] In response, the FTC argued that Wyndham had received rather robust notice.[145] Specifically, the FTC argued that Wyndham received notice of the Commission's data security requirements by means of the complaints and consent decrees from other FTC data security enforcement actions, which the FTC publishes on its website.[146] Additionally, the FTC contended that many of the inadequate practices that

137. *See* discussion *supra* notes 117–20 and accompanying text.

138. Respondent LabMD, Inc.'s Answer and Defenses to Administrative Complaint at 7, *LabMD, Inc.*, No. 9357, https://www.ftc.gov/sites/default/files/documents/cases/2013/09/110917labmdanswer.pdf [https://perma.cc/562Z-ADG9].

139. Solove & Hartzog, *supra* note 7, at 610–11. As of this writing, a disposition on the merits is still pending. *See LabMD, Inc., in the Matter of*, FED. TRADE. COMM'N (Feb. 5, 2016), https://www.ftc.gov/enforcement/cases-proceedings/102-3099/labmd-inc-matter [https://perma.cc/3PP7-PN4N].

140. *See* FTC v. Wyndham Worldwide Corp., 799 F.3d 236, 240 (3d Cir. 2015).

141. *Id.* (quoting Complaint at ¶ 24, FTC v. Wyndham Worldwide Corp., 10 F. Supp. 3d 602 (D.N.J. 2014) (No. 13-1887(ES))).

142. *Id.* at 240–41.

143. *See id.* at 241–42.

144. *See id.* at 240. Wyndham also argued that the FTC lacked the statutory authority under the unfairness prong of section 5 to regulate data security. *See id.* Regarding this issue, the court held that data security practices can fall within the plain meaning of "unfair" under section 5 and that congressional action after the enactment of section 5 had not preempted that statute's use in the context of data security. *See id.* at 248–49.

145. *See* Brief for Plaintiff-Appellee at 40–52, *Wyndham*, 799 F.3d 236 (No. 14-3514), https://www.ftc.gov/system/files/documents/cases/141105wyndham_3cir_ftcbrief.pdf [https://perma.cc/8U4G-W9S5].

146. *See id.* at 45–52.

Wyndham had in place were addressed in a widely available FTC guide[147] published before Wyndham suffered its first data security breach.[148]

The court stated that, where an entity can reasonably foresee that its conduct violates a statute, there is constitutionally adequate notice.[149] As Wyndham had access to publically available FTC complaints filed against other companies that had similarly inadequate data security practices and FTC statements regarding data security generally, in addition to the fact that it had suffered "not one or two, but three" data security breaches, the court held that, as applied to Wyndham, there was constitutionally adequate notice.[150]

In sum, *LabMD* and *Wyndham* provide recent examples of overarching concerns that the FTC has not provided companies with sufficient guidance as to what it considers to be "reasonable" data security practices for purposes of section 5 enforcement.[151] This Note now turns to consider scholarly proposals that have sought to give substance to the FTC's data security requirements, specifically as they relate to enforcement actions relying on the FTC's unfairness authority.

III. WAIT, WHAT'S REASONABLE?: PROPOSED SOLUTIONS TO THE FTC'S FAILURE TO PROVIDE ADEQUATE NOTICE OF WHAT IT DEEMS TO BE UNFAIR DATA SECURITY PRACTICES

In light of the FTC's arguably vague complaints and the relative lack of case law or other guidance regarding what constitutes sufficient data security measures under the FTC's unfairness authority, there is a sense in the legal community that the FTC has not provided sufficient guidance to companies regarding what "reasonable" or "adequate" data security measures they should implement.[152] This part considers and provides a critical analysis of proposals to promote a data security enforcement regime

147. *See generally* FED. TRADE COMM'N, PROTECTING PERSONAL INFORMATION: A GUIDE FOR BUSINESS (2011), https://www.ftc.gov/system/files/documents/plain-language/bus69-protecting-personal-information-guide-business_0.pdf [https://perma.cc/39X8-ZZ5Q]. A version of this guide was available in 2007. *See* Brief for Plaintiff-Appellee, *supra* note 145, at 49.

148. *See* Brief for Plaintiff-Appellee, *supra* note 145, at 49–52.

149. *See Wyndham*, 799 F.3d at 256.

150. *See id.* at 256–59. Despite the Third Circuit's holding that Wyndham received fair notice, this Note argues that, even if the FTC has given constitutionally adequate notice, as a policy matter it still has not given sufficient notice to regulated entities regarding its minimum data security requirements. *See infra* Part IV.A. In December 2015, Wyndham settled with the FTC. *See* Press Release, Fed. Trade Comm'n, Wyndham Settles FTC Charges It Unfairly Placed Consumers' Payment Card Information at Risk (Dec. 9, 2015), https://www.ftc.gov/news-events/press-releases/2015/12/wyndham-settles-ftc-charges-it-unfairly-placed-consumers-payment [https://perma.cc/C9UK-VZ2L]; *see also supra* note 78.

151. *See supra* notes 128–29 and accompanying text.

152. *See, e.g.*, Scott, *supra* note 10, at 143–44; Serwin, *supra* note 21, at 812–13; Stegmaier & Bartnick, *supra* note 6, at 676. *But see* Solove & Hartzog, *supra* note 7, at 589 (arguing that the FTC's enforcement actions essentially have created a new area of privacy common law).

that better informs companies of those data security practices that the FTC deems "unfair."

A. Proposed Solutions

At present, there are multiple perspectives on this issue, which this Note broadly characterizes as: (1) the ad hoc approach; (2) the legislative fix; (3) the administrative fix; and (4) a proposal for a new privacy framework. Each of these is discussed in turn.[153]

1. The Ad Hoc Approach

With respect to notifying companies of its data security requirements, the FTC has, until now, engaged in an essentially ad hoc, enforcement-based approach.[154] Relying upon adjudication to advance its data security policy,[155] the FTC publishes complaints and consent orders from enforcement actions regarding inadequate data security practices on its website.[156] The Commission contends that, by providing companies with documents from past data security enforcement actions listing specific practices that violate section 5, it adequately notifies those companies of its evolving data security requirements.[157] Additionally, the FTC notes that it publishes various online guidance brochures discussing data security best practices.[158] The FTC also has begun hosting live "Start with Security" events, which enable the FTC "to provide companies with practical tips and strategies for implementing effective data security."[159]

---

153. Scholars have noted that there is a "dearth of scholarship" in this area. Solove & Hartzog, *supra* note 7, at 588. Therefore, there is not an extensive body of literature for this Note to review. Nevertheless, the relative scholarly silence regarding such a pressing societal issue serves to underscore the importance of this Note's thesis.

154. *See* Stegmaier & Bartnick, *supra* note 6, at 692.

155. Under *SEC v. Chenery Corp.*, the FTC can opt to promulgate policy via adjudication. *See supra* notes 51, 68.

156. *See, e.g.*, *BJ's Wholesale Club, Inc., in the Matter of*, FED. TRADE COMM'N (Sept. 23, 2005), https://www.ftc.gov/enforcement/cases-proceedings/042-3160/bjs-wholesale-club-inc-matter [https://perma.cc/68FD-9DWM]; *Dave & Buster's, Inc., in the Matter of*, FED. TRADE COMM'N (June 8, 2010), https://www.ftc.gov/enforcement/cases-proceedings/082-3153/dave-busters-incin-matter [https://perma.cc/X645-J3P2]; *TJX Companies, the, Inc., in the Matter of*, FED. TRADE COMM'N (Aug. 1, 2008), https://www.ftc.gov/enforcement/cases-proceedings/072-3055/tjx-companies-inc-matter [https://perma.cc/2WZN-TCWY].

157. *See, e.g.*, Brief for Plaintiff-Appellee, *supra* note 145, at 45–49.

158. *See, e.g.*, *id.* at 49–52. For examples of such guidance, see FED. TRADE COMM'N, *supra* note 147; FED. TRADE COMM'N, START WITH SECURITY: A GUIDE FOR BUSINESS (2015), https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf [https://perma.cc/H8JT-SRRW]. The FTC also has a webpage dedicated to data security. *See Data Security*, FED. TRADE COMM'N, https://www.ftc.gov/tips-advice/business-center/privacy-and-security/data-security (last visited Mar. 27, 2016) (providing links to videos and other FTC webpages with data security-related guidance) [https://perma.cc/HBX7-GZ8X].

159. *Start with Security—Austin*, FED. TRADE COMM'N, https://www.ftc.gov/news-events/events-calendar/2015/11/start-security-austin (last visited Mar. 27, 2016) (describing one such event in Austin, Texas) [https://perma.cc/3WQ5-A4ZT].

Professors Daniel Solove and Woodrow Hartzog argue that the FTC's current practice is on the right track.[160] While discussing the FTC's role in privacy enforcement generally, they have argued that the FTC has essentially developed a body of privacy "common law" through their various complaints, consent orders, and guidance materials, which, when considered as a whole, constitute a robust body of online privacy and data security jurisprudence.[161]

More specifically, Solove and Hartzog contend that the FTC's many data security complaints and consent orders are the functional equivalent of judicial common law, not only because the orders are published on the FTC's website and the Commission typically follows a given order in subsequent enforcement actions, but also because lawyers look to these documents when advising corporate clients on data security matters.[162] Additionally, the authors liken other materials published by the FTC regarding its data security requirements—such as press releases and online guidance[163]—to dicta in judicial opinions, as they, too, provide some sense of what the FTC requires of companies in terms of minimum data security requirements.[164]

Solove and Hartzog go on to argue that the FTC has developed overarching principles within its privacy and data security "jurisprudence."[165] For instance, mimicking the incremental development of common law,[166] the FTC has begun requiring through its data security enforcement actions that companies follow ever more specific data security standards.[167] In response to the argument that the FTC does not adequately notify companies of its minimum data security requirements, the authors provide a list of twenty-five "standards" identified in data security-related complaints and consent orders.[168] Thus, according to the authors, the FTC's data security jurisprudence provides ample notice of its data security expectations.[169]

In addition, Solove and Hartzog argue that the FTC's data security jurisprudence has provided companies with a "baseline" to follow.[170] Drawing from established industry norms and resulting consumer

160. *See* Solove & Hartzog, *supra* note 7, at 589. Although the article addresses the FTC's involvement in privacy enforcement generally, the authors do spend considerable time discussing the FTC's data security jurisprudence. *See id.* at 650–55 (explaining the specific data security practices that the FTC has identified by means of data security enforcement cases).

161. *See id.* at 585–86.

162. *See id.* at 621–22.

163. *See supra* notes 157–58 and accompanying text.

164. *See* Solove & Hartzog, *supra* note 7, at 626.

165. *See id.* at 627. With regard to the FTC's data security jurisprudence under its unfairness authority, Solove and Hartzog's discussion is limited to the most general of terms. *See id.* at 643 ("[T]he FTC deem[s] . . . defendants' lack of adequate security measures to be an unfair practice.").

166. *See id.* at 648.

167. *See id.* at 590.

168. *See id.* at 650–55.

169. *See id.* at 650–51.

170. *See id.* at 661.

expectations, the authors suggest that the FTC has demanded "adequate data security" as a requirement to avoid liability under the unfairness prong of section 5.[171]

In light of the FTC's growing privacy and data security jurisprudence, Solove and Hartzog call upon the FTC to continue drawing from industry norms, as well as the consumer expectations those norms created, to give ever more substance to its requirement that companies employ "reasonable" data security measures.[172] Moreover, they suggest that the FTC should be emboldened to continue enforcing data security breaches under the unfairness authority of section 5.[173]

2. The Legislative Fix

In contrast to those who believe that the FTC's current practice is best, at least one scholar would rely on Congress to provide a direct statutory grant of authority to the FTC to enforce unfair data security practices.[174] For example, Professor Michael D. Scott has maintained that, because the FTC has neither provided for hearings or public comment nor promulgated legislative or nonlegislative rules, companies have received no real guidance as to which data security practices the FTC deems to be unfair.[175] Indeed, Scott has gone further by suggesting that the FTC may be exceeding its statutory authority by bringing its unfairness authority to bear on companies that suffer data security breaches.[176] By applying the three-pronged test required for a finding of unfairness under section 5[177] to extant FTC data security cases, he has sought to show that allegations of unfairness against companies that suffered data security breaches do not pass statutory muster.[178]

As to substantial injury, Scott notes that FTC data security cases relying on an unfairness theory contain no allegations of substantial monetary loss.[179] The FTC argues that consumers are substantially injured to the extent that they are inconvenienced by having to deal with identity theft and that there is significant monetary injury when the total amount of fraudulent

171. *Id.* at 661–62.

172. *See id.* at 673.

173. *See id.* at 676. The article concludes by suggesting that there is more room for the FTC's data security jurisprudence to be fleshed out. *See id.* ("This Article is hopefully the start of a more sustained examination of the FTC, the body of [privacy] law it has developed, and the future directions that law can take."). This Note intends to be a step in that direction.

174. *See* Scott, *supra* note 10, at 183.

175. *See id.* at 143–44.

176. *See id.* at 129. Professor Scott's article was written before the Third Circuit held that inadequate data security practices could lead to a finding of unfairness for the purposes of section 5. *See supra* note 144.

177. *See supra* notes 56–57 and accompanying text. For reference, the FTC must show that consumer injury was: (1) substantial; (2) not outweighed by any countervailing benefits to consumers or competition; and (3) an injury that consumers themselves could not reasonably have avoided. *See* 15 U.S.C. § 45(n) (2012).

178. *See* Scott, *supra* note 10, at 151–65.

179. *See id.* at 153.

purchases made by identity thieves is aggregated.[180] Scott maintains, however, that these are not actionable injuries under section 5 because there is no showing of an actual, specific, monetary loss to consumers.[181]

Looking to the next prong of the three-part test for a finding of unfairness, Scott notes that companies must strike a balance between having no data security, which is certainly unreasonable, and perfect security, which is unachievable.[182] However, as the FTC has not provided for hearings or public comment regarding unfair data security practices, he explains that there is no way for companies realistically to strike that balance.[183] Thus, Scott concludes, the FTC cannot accurately determine whether injuries are outweighed by benefits to competition or consumers.[184]

Lastly, Scott considers consumers' ability to avoid being exposed to a data security breach.[185] As it would be patently unreasonable to require that consumers refrain from things such as using credit cards, Scott determines that the third prong required for a finding of unfairness would weigh in the FTC's favor.[186]

Based on the foregoing analysis, Scott suggests that the FTC has exceeded its statutory authority under section 5 by bringing unfairness cases against companies who have suffered data security breaches.[187] Accordingly, he proposes an overarching legislative fix that would explicitly direct the FTC to regulate corporate data security.[188]

With respect to specifics, in addition to granting the FTC jurisdiction over data security under section 5, Scott's proposed legislation would require the FTC to promulgate legislative rules directing companies to implement "policies and procedures regarding information security practices."[189] Notably, this rulemaking authority would lack the additional procedural burdens currently in place under section 5.[190] Finally, the proposed statute would explicitly state that the FTC's enforcement authority

180. *See id.* at 157.
181. *See id.*
182. *See id.* at 160.
183. *See id.*
184. *See id.*
185. *See id.* at 161–62.
186. *See id.* Scott also argues that the FTC's use of its unfairness authority against companies that have suffered data security breaches is questionable at best because there is no "clearly established" public policy regarding data security breaches. *See id.* at 162–65.
187. *See id.* at 183. As a result, according to Scott, a company subject to data security breaches must now chose either to avoid competing in sectors where consumer data could be compromised or overinvest in new technology to ensure compliance with the FTC's requirements. *See id.* at 171.
188. *See generally id.* at 177–82. For his proposal, Scott draws on other statutes that give the FTC industry-specific jurisdiction over certain data security breaches. *See id.* at 172.
189. *Id.* at 178. Under Scott's proposal, the FTC will explicitly look to "generally accepted national and international information security standards" to give substance to its requirements. *Id.* at 179.
190. *See id.* at 178 (requiring that the FTC follow 5 U.S.C. § 553 (2012) when promulgating rules under the proposed statute); *see also supra* notes 66–67 and accompanying text (discussing the procedural burdens currently in place under section 5).

vis-à-vis data security breaches is derived from section 5 itself.[191] Ultimately, Scott's goal is to ensure that companies know what the FTC considers to be unfair data security practices so that they can implement proper security measures to adequately protect consumer data.[192]

3. The Administrative Fix

Also in opposition to the FTC's current practices, others contend that the FTC should exercise its administrative authority by promulgating regulations that detail what it expects of companies in terms of data security practices.[193] Put another way, these scholars would have the FTC issue data security guidance via legislative or nonlegislative rulemaking.[194] Two attorneys who specialize in information privacy practice, Gerard Stegmaier and Wendell Bartnick, have offered such a proposal.[195]

Much like Professor Scott, Stegmaier and Bartnick argue that the FTC has provided little ascertainable guidance to companies regarding which data security practices it considers unfair.[196] The authors explain that the FTC has contented itself with providing notice to companies via its published complaints and consent decrees and its online data security reports.[197] This general practice, to the authors, is not enough to provide adequate notice[198] because it does nothing more than explain that certain "unreasonable" practices "taken together" add up to liability under the FTC's unfairness authority.[199]

In response to the FTC's current practice, Stegmaier and Bartnick suggest that the FTC ought to engage in legislative rulemaking that

---

191. *See* Scott, *supra* note 10, at 180. In addition to making the FTC's data security enforcement authority explicit, Scott notes that his statute would provide the added benefit of allowing for public input during the rulemaking process. *See id.* at 183.

192. *See id.* As of this writing, there is data security legislation pending before the Senate. *See* Data Security and Breach Notification Act of 2015, S. 177, 114th Cong. (2015). This bill grants the FTC specific authority to regulate data security breaches under section 5. *See id.* § 5(c)(1). However, the bill appears to grant the FTC the same rulemaking authority that is has under section 5. *See id.* § 5(c)(2). In other words, the FTC would be subject to the same onerous rulemaking procedures as it is under section 5 already. *See supra* note 66 and accompanying text.

193. *See* Stegmaier & Bartnick, *supra* note 6, at 720.

194. *See id.*; *see also supra* Part I.B.3.

195. *See* Stegmaier & Bartnick, *supra* note 6, at 720. The authors suggest that the FTC has not provided constitutionally adequate notice to companies of which data security practices it considers to be unfair. *See id.* at 706. It bears repeating that, after they published their article, the Third Circuit held that, at least as applied, the FTC *has* adequately provided companies with such notice. *See* FTC v. Wyndham Worldwide Corp., 799 F.3d 236, 256–59 (3d Cir. 2015); *see also supra* note 150 and accompanying text.

196. *See* Stegmaier & Bartnick, *supra* note 6, at 695.

197. *See id.* at 691–94. The authors do note that, under *SEC v. Chenery Corp.*, the FTC has the discretion to choose to promulgate policy via adjudication rather than rulemaking. *See* Stegmaier & Bartnick, *supra* note 6, at 691.

198. *See id.* at 695. Indeed, Stegmaier and Bartnick maintain that "[e]ven if the FTC has provided enough notice to meet constitutional requirements, . . . its current efforts are inadequate." *Id.* at 676.

199. *See id.* at 691–93.

explicitly lays out what it considers to be unfair data security practices.[200] First, the authors note that the FTC already has successfully engaged in data security-based legislative rulemaking under certain industry-specific statutes which grant the FTC express authority to enforce data security breaches.[201] Given these successes, Stegmaier and Bartnick argue that the legislative rulemaking process under section 5 itself would be beneficial because it would provide notice to regulated companies via the required notice-and-comment period and allow companies to provide input toward any proposed rule.[202] Additionally, the authors claim that specific guidance as to the FTC's minimum data security requirements provided in a legislative rule would prevent companies from overinvesting in unnecessary data security measures in an effort to avoid liability.[203] With respect to the onerous procedural requirements for legislative rulemaking under section 5,[204] Stegmaier and Bartnick maintain that the costs of the rulemaking process will be outweighed by the savings derived from increased industry compliance, which would be spurred by clearer, more ascertainable data security requirements.[205] Aside from legislative rulemaking, Stegmaier and Bartnick also suggest that nonlegislative rules, in whichever form, that more specifically outline what the FTC considers to be unfair data security practices, may also serve to provide improved notice to companies as against the FTC's current practices.[206]

Stegmaier and Bartnick recommend that any rule, legislative or nonlegislative, that the FTC promulgates *must* be more specific than the FTC's current reasonableness requirement.[207] To these authors, adequate notice requires more practical requirements that help companies understand what data security practices would be considered "unfair" for the purposes of section 5.[208]

4. A Proposal for a New Privacy Framework

Lastly, Andrew Serwin, an attorney who practices in the areas of privacy and cybersecurity, has proposed an entirely new framework for privacy

200. *See id.* at 707. Stegmaier and Bartnick also suggest that the FTC, in lieu of or in addition to legislative rulemaking, should continue to engage in formal adjudication and litigation. *See id.* at 714–15. According to the authors, these processes would provide greater notice to regulated companies than the FTC's current practices because they would receive, in the case of formal adjudication, more specific FTC findings of facts and, in the case of litigation, judicial decisions on the merits regarding violations of section 5. *See id.*

201. *See id.* at 708.

202. *See id.* at 710–11.

203. *See id.*; *see also supra* note 187.

204. *See supra* notes 66–67 and accompanying text.

205. *See* Stegmaier & Bartnick, *supra* note 6, at 712. Moreover, the authors contend that the FTC will see additional savings in investigation and litigation costs because clearer data security rules would make it easier for the Commission to identify and enforce unfair data security practices. *See id.*

206. *See id.* at 715–17.

207. *See id.* at 717–20; *see also supra* notes 199–200 and accompanying text.

208. *See* Stegmaier & Bartnick, *supra* note 6, at 717.

enforcement in the United States.[209] In his article, he notes that the notice-and-choice[210] and the harm-based models[211] have failed to engender effective enforcement.[212] He then goes on to discuss three distinct "models for privacy,"[213] which include the accountability model,[214] processing limitations model,[215] and proportionality model.[216]

Serwin defines the accountability model of privacy as a regime in which companies are held accountable for how they handle consumer data.[217] In his view, this model relies heavily upon reactive and involuntary privacy enforcement.[218] While he deems enforcement to be an important part of any privacy regime, Serwin does not consider it to be the appropriate focal point because any regime based primarily upon enforcement leaves regulated entities without any meaningful ex ante guidance.[219]

Serwin next considers the processing limitations model, which he explains has its focus on restricting the use of information.[220] As with the accountability model, he maintains that this model, while important, cannot be the focus of a privacy regime because any restrictions on data usage should be based on an ascertainable governing principle.[221]

Lastly, to provide privacy regulation with a governing principle, Serwin discusses a proportionality-based privacy model,[222] which relies on the premise that privacy safeguards should be related to the sensitivity of the data they are meant to protect.[223] Under this regime, Serwin would propose a four-tiered framework—ranging from "nonsensitive" to "highly sensitive"—that would categorize specific types of data by sensitivity.[224] Thus, Serwin's proposal would define how sensitive a given type of consumer information is and attach to that categorization an attendant set of security requirements based upon industry best practices.[225] This approach, Serwin argues, would govern both the limitations on the use of data and the

209. *See* Serwin, *supra* note 21, at 812–13.
210. *See supra* notes 94–95 and accompanying text.
211. *See supra* notes 102–03 and accompanying text.
212. *See* Serwin, *supra* note 21, at 842–44. Serwin also notes that the FTC itself has recognized that these models have been somewhat ineffective. *See id.* at 843.
213. *See id.* at 844.
214. *See id.*
215. *See id.* at 848.
216. *See id.* at 849.
217. *See id.* at 846.
218. *See id.*
219. *See id.* at 848 ("[A]n accountability-centric model would be like passing comprehensive privacy legislation and simply saying, 'If you violate someone's privacy you will be liable for a $10,000 fine,' without defining what data is covered or what acts are prohibited.").
220. *See id.*
221. *See id.* at 849 ("[A process limitations-centric model] would be like passing legislation that provides restrictions on the use of data without defining data in the first place.").
222. *See id.*
223. *See id.* at 852.
224. *See id.* at 850.
225. *See id.* at 851.

appropriate means of enforcement based upon the sensitivity of the data in question.[226]

Serwin goes on to outline a number of benefits to a proportionality-based privacy model.[227] For example, he notes that a preexisting tier system would serve to protect consumer information ex ante by enabling companies to use data security practices to prevent breaches rather than relying on ex post enforcement.[228] Additionally, Serwin explains that his proposed framework would provide administrative flexibility as any given type of information could be moved between tiers.[229] Serwin also contends that this regime would help provide guidance to companies so that they could know, at the outset, where a given dataset falls on the sensitivity continuum.[230]

With respect to implementation, Serwin expresses ambivalence as between administrative rulemaking and legislation.[231] In either case, he would encourage the development of a new regime wherein the FTC would administer a voluntary, proportionality-based program that would seek to encourage companies to implement best practices.[232] Compliance with this regime would provide a safe harbor, immunizing compliant companies from enforcement actions.[233]

B. A Critical Analysis of Proposed Solutions

Although each of the proposals discussed in Part III.A has its merits, this Note contends that there is room for improvement. Part III.B analyzes each of the proposals discussed in Part III.A in light of important societal interests. As noted above,[234] these interests include the need for better notice to regulated entities,[235] the FTC's goal of robust consumer protection,[236] and the FTC's need for administrative flexibility given the ever-evolving technological environment that it is regulating.[237]

1. The Ad Hoc Approach

Advocates of the ad hoc approach, such as the FTC itself along with Solove and Hartzog, believe that the FTC's current strategy, which focuses on enforcement and relies upon published complaints, consent orders, and online guidance to provide notice, adequately informs companies of the FTC's minimum data security requirements.[238] This Note argues that, at

226. *See id.* at 850.
227. *See id.* at 851–52.
228. *See id.* at 851.
229. *See id.*
230. *See id.* at 852.
231. *See id.* at 854.
232. *See id.* at 812–13.
233. *See id.*
234. *See supra* notes 19–21 and accompanying text.
235. *See, e.g.*, Stegmaier & Bartnick, *supra* note 6, at 706–07.
236. *See What We Do*, *supra* note 20.
237. *See* Serwin, *supra* note 21, at 852.
238. *See supra* notes 154–59 and accompanying text.

least as to consumer protection and notice to regulated companies, this approach falls short.

The ad hoc approach does provide the FTC with a great deal of administrative flexibility. As it can opt to promulgate policy via adjudication,[239] this approach enables the FTC to pick and choose which data security breaches to enforce. Thus, through enforcement, the FTC can continue to bring actions against companies that it deems to have engaged in "unfair" data security practices.[240]

As to consumer protection, the ad hoc approach provides robust ex post protection. In other words, after a security breach occurs, the FTC will bring an enforcement action against a company if it believes the company employed "unfair" data security practices.[241] While this strategy may well vindicate certain consumers' injuries, it ignores robust ex ante protection, which would serve to protect consumers before a data security breach occurs by ensuring that companies have the proper incentives to employ data security best practices.[242] The benefit of ex ante protection is that it helps to prevent the very breaches that the FTC enforces.

This approach also fails to provide adequate notice to companies of which practices the FTC considers "unfair." The FTC's complaints and consent orders merely list data security practices that, "taken together," add up to unfair practices.[243] While the FTC's online guidance is a step in the right direction,[244] it lacks the specifics necessary to ensure that companies know exactly what they need to do to avoid liability under the FTC's unfairness authority.

These shortcomings are illustrated well by the case against Wyndham.[245] If Wyndham had been provided ex ante notice of which data security practices it needed to implement to comply with FTC standards, it could have ensured that it had proper data security measures in place to better protect consumer information.[246]

Solove and Hartzog contend that the FTC's complaints and consent orders provide a great deal of standards, which illustrate that the FTC, as a baseline, requires companies to employ "adequate data security [practices]."[247] However, this baseline still forces companies to ask, "Which of the practices required of the respondent company in any given enforcement action are required of *my* company?"

---

239. *See supra* notes 51, 68, 155.

240. *See supra* Part II.B (discussing the FTC's use of its unfairness authority in the data security context).

241. *See supra* Part II.B.

242. *See supra* notes 219, 228 and accompanying text.

243. *See, e.g.*, *supra* note 141 and accompanying text.

244. *See supra* note 158 (providing examples of such guidance).

245. *See supra* notes 140–50 and accompanying text.

246. *See infra* Part IV.A.

247. *See* Solove & Hartzog, *supra* note 7, at 661–62; *see also supra* notes 165–71 and accompanying text.

2. The Legislative Fix

Professor Scott argues that Congress must enact a statute to enable the FTC to police data security breaches under section 5.[248] This Note takes the view that this proposal fails to provide sufficient administrative flexibility.

First, Scott's proposal would resolve the current lack of notice to companies regarding the FTC's minimum data security requirements. His proposed statute would require the FTC to engage in legislative rulemaking with respect to data security requirements under section 5.[249] This requirement would ensure that companies would receive improved notice, through both the notice-and-comment period and the promulgation of any final rule,[250] of which data security practices the FTC deems "unfair."

Relatedly, this proposal would have the benefit of providing for ex ante and ex post consumer protection. Any rules promulgated pursuant to Scott's proposed statute would give regulated companies a better understanding of which practices the FTC considers unfair.[251] Thus, they would be able to employ these practices and better protect consumer information before a breach occurs.[252] Moreover, Scott's statute would provide enforcement authority under section 5,[253] so those companies that fail to follow the FTC's requirements would be held accountable as they are today.[254]

Although Scott's proposal maximizes consumer protection and notice to companies, it does not ensure sufficient administrative flexibility. His proposed statute would require the FTC to issue any legislative rules by following the procedures set forth in the APA.[255] While this process would evade the added procedural obstacles in place under section 5,[256] it would make any promulgated final rules difficult to amend and adjust in light of changing technology. Moreover, actually getting any proposed rules through the notice-and-comment period required under the APA would be quite expensive for the FTC in terms of time and money. Given these onerous obstacles, this proposal would make it rather difficult for the FTC to give companies like Wyndham robust notice of its data security requirements.

---

248. *See supra* Part III.A.2.
249. *See supra* note 189 and accompanying text.
250. *See supra* notes 64–65 and accompanying text.
251. *See supra* note 189 and accompanying text.
252. *See supra* note 228 and accompanying text.
253. *See supra* note 191 and accompanying text.
254. *See supra* Part II.B (explaining how the FTC brings its unfairness authority to bear upon companies that suffer data security breaches).
255. *See supra* notes 64–65 and accompanying text.
256. *See supra* note 66 and accompanying text (outlining the procedural requirements under section 5).

3. The Administrative Fix

In contrast to Professor Scott, Stegmaier and Bartnick argue that the FTC should use its administrative authority under section 5 to provide better notice of its minimum data security requirements.[257] This Note contends that, to the extent that the proposal would require that the FTC engage in legislative rulemaking, it likely would not provide for adequate administrative flexibility.

Stegmaier and Bartnick's proposal would afford regulated companies improved notice as against the FTC's current practice.[258] They maintain that the FTC should, preferably, engage in legislative rulemaking to set out its data security requirements.[259] However, they also note that nonlegislative rulemaking (e.g., issuing policy statements or interpretive rules) would be better than nothing.[260] In either case, any promulgated rule would have the benefit of providing notice to companies as to which data security practices the FTC considers "unfair."[261]

Additionally, Stegmaier and Bartnick's proposal would lead to significantly improved consumer protection. Ex ante, their proposal would provide guidance to companies via promulgated rules.[262] In turn, these companies could employ data security best practices to ensure the data security breaches are less likely to occur.[263] Ex post, section 5 enforcement would remain in place to enable the FTC to hold companies who failed to implement required data security practices accountable.[264]

Despite these benefits, Stegmaier and Bartnick's proposal may not provide the FTC with adequate administrative flexibility. The authors explicitly prefer legislative rulemaking, as that process would provide additional notice to companies via notice and comment and the required informal hearing procedure.[265] However, putting aside difficulties in getting any proposed rule through the hearing and notice-and-comment procedures,[266] such a process would make it rather difficult to amend any rule regarding data security practices. Such flexibility is invaluable in light of the dynamic technological environment in which data security enforcement takes place.[267] Indeed, under this proposal, the FTC would have to adopt a new legislative rule every time it needed to adjust its data

257. *See supra* Part III.A.3.
258. *See supra* notes 202–03 and accompanying text.
259. *See supra* note 200 and accompanying text.
260. *See supra* note 206 and accompanying text.
261. *See supra* notes 207–08 and accompanying text.
262. *See supra* notes 207–08 and accompanying text.
263. *See supra* note 200 and accompanying text.
264. *See supra* Part II.B (discussing how the FTC brings its unfairness authority to bear upon companies that suffer data security breaches).
265. *See* Stegmaier & Bartnick, *supra* note 6, at 710 ("[Legislative] [r]ulemaking likely is the best method for providing authoritative, detailed guidance so that entities know how to comply with the law.").
266. *See supra* notes 66–67 and accompanying text.
267. *See supra* note 21 and accompanying text.

security requirements to give appropriate ex ante guidance to companies such as Wyndham. This would be a significant burden for the FTC.

4. A Proposal for a New Privacy Framework

Lastly, this Note addresses Serwin's proposal for a new privacy framework in which the FTC would administer a regime based upon proportionality that provides a safe harbor from enforcement for compliant companies.[268] Although this approach would likely do the most to maximize consumer protection and notice to companies, it may not ensure sufficient administrative flexibility.

Like the legislative and administrative approaches,[269] Serwin's proposal would provide improved notice to companies. Be it via legislation or rulemaking, this proposal would ensure that regulated companies know the FTC's data security requirements.[270] Moreover, Serwin's four-tiered approach has the added benefit of providing nuanced guidance as to how companies can protect consumer information based on its relative sensitivity.[271]

This improved notice would serve to promote consumer protection as well. First, Serwin's proposal incentivizes companies to adopt data security best practices as outlined by the FTC because, in so doing, they avoid liability under section 5.[272] Thus, from an ex ante perspective, companies would be better able to prevent data security breaches from occurring.[273] Furthermore, this proposal enables the FTC to engage in ex post enforcement by bringing actions against those companies that fail to adopt data security best practices.[274]

With respect to administrative flexibility, however, Serwin's proposal would seem to come up short. In his article, Serwin expresses ambivalence about implementing his proposal via legislation or rulemaking.[275] Either process, however, could undercut flexibility. Rulemaking would place procedural obstacles before the FTC because any amendments to rules promulgated under Serwin's proposal would need to go through notice and comment and section 5's onerous procedural requirements.[276] Moreover, any legislation would prove to be exceedingly inflexible because the FTC would need to rely on Congress to amend a statute to provide it with the flexibility to address new and evolving data security threats.

Serwin argues that his approach is flexible because it would enable the FTC to move a given type of consumer information to a different tier in his

268. *See supra* Part III.A.4.
269. *See supra* Part III.A.2–3.
270. *See supra* note 228 and accompanying text.
271. *See supra* notes 224–25 and accompanying text.
272. *See supra* note 233 and accompanying text.
273. *See supra* note 228 and accompanying text.
274. *See supra* note 233 and accompanying text.
275. *See supra* note 231 and accompanying text.
276. *See supra* notes 64–67 and accompanying text.

four-tiered framework.[277] While this may well be true, Serwin seems to ignore the fact that implementation via legislation or rulemaking would require any changes to be implemented via the same onerous processes. Thus, as is the case with the other proposals, the FTC could not provide companies like Wyndham with adequate notice of its data security requirements without dealing with significant procedural hurdles.

IV. TOWARD A REASONABLE REGIME: A NEW PROPOSAL REGARDING THE FTC'S CURRENT APPLICATION OF ITS UNFAIRNESS AUTHORITY IN THE DATA SECURITY CONTEXT

As Part III.B demonstrates, current proposals regarding the FTC's use of its unfairness authority in the data security context fail to maximize consumer protection, administrative flexibility, and notice to regulated companies. Accordingly, in an effort to maximize each of these important societal interests, Part IV.A of this Note proposes a new solution to the lack of clarity in the FTC's data security jurisprudence and discusses its benefits and an identified drawback. Then, Part IV.B considers a potential drawback to this Note's novel proposal.

A. A New Proposal Incorporating the Principle of Proportionality

In terms of implementation, the FTC should issue the following proposal by means of nonlegislative rulemaking.[278] As outlined above, this form of rulemaking could take the form of an interpretive rule or a policy statement.[279] An interpretive rule could outline how the FTC interprets section 5 with respect to unfair data security practices.[280] Alternatively, a policy statement could notify regulated companies and the public generally of the manner in which the FTC will exercise its unfairness authority in the data security context moving forward.[281]

Delineating the exact data security practices that the FTC should outline in any nonlegislative rulemaking is beyond the scope of this Note. However, Solove and Hartzog's article seems to provide a sufficient starting point. Upon analyzing "the FTC's data security jurisprudence," the authors compiled a list of what they term "inadequate security practices."[282] For instance, Solove and Hartzog note that, in publically available complaints and consent orders, the FTC appears to deem such things as "[l]ack of encryption," "[f]ail[ing] to test the security of a . . . process," "[f]ail[ing] to remedy known security vulnerabilities," "[f]ail[ing] to implement . . . common industry security practices," and "[the use of] [p]oor username/password protocol" to be unfair data security practices per se.[283] Accordingly, the FTC should draw from Solove and Hartzog's work

277. *See supra* note 229 and accompanying text.
278. *See supra* note 69 and accompanying text.
279. *See supra* note 70 and accompanying text.
280. *See supra* note 71 and accompanying text.
281. *See supra* note 72 and accompanying text.
282. Solove & Hartzog, *supra* note 7, at 651.
283. *Id.* at 650–55.

and look to its own complaints and consent orders[284] to determine which data security practices it considers "unfair."

The FTC should not stop there. As Serwin's article indicates, not all consumer information should be subject to the same data security requirements.[285] Some companies possess rather sensitive personal information (e.g., Social Security numbers and fingerprint data), while others have more mundane information (e.g., usernames and email addresses). Thus, any nonlegislative rulemaking should incorporate the principle of "proportionality."[286] Drawing from Serwin, the FTC should determine where a given type of consumer information falls on the spectrum between "nonsensitive" and "highly sensitive."[287] For example, the FTC could itemize types of consumer data under categories, such as Schedules I through IV, where Schedule I includes the least sensitive consumer information, while Schedules II, III, and IV include increasingly more sensitive information. The FTC then could ratchet up the minimum data security requirements for those companies with more sensitive consumer information.[288] To be most effective, any nonlegislative rulemaking should also lay out what minimum data security practices correspond with each schedule (i.e., "tier") of consumer information.[289] Under such a regime, companies will know, based on the types of consumer information that they retain, which data security practices they ought to have in place.

Lastly, as Serwin has proposed, the FTC should include a safe harbor provision in its nonlegislative rulemaking promulgated pursuant to this Note's proposal.[290] Such a provision would state explicitly that any company that complies with the data security requirements as laid out in the interpretive rule or policy statement would be deemed to have acted "fairly" for the purposes of section 5.[291] Accordingly, a regulated company would know, ex ante, whether its data security practices are in compliance with section 5.[292]

This Note's proposal would serve to maximize notice to companies, consumer protection, and administrative flexibility. First, it would improve notice to companies. By outlining, as specifically as possible, which data security requirements correspond with specific types of consumer information,[293] a company would know what the FTC requires of it in terms

284. *See supra* note 156 and accompanying text.
285. *See supra* notes 222–23 and accompanying text.
286. *See supra* notes 222–23 and accompanying text.
287. *See supra* note 224 and accompanying text.
288. *See supra* note 225 and accompanying text.
289. *See supra* note 225 and accompanying text.
290. *See supra* note 233 and accompanying text.
291. In the context of corporate compliance, there is a similar regime wherein the U.S. Sentencing Commission has required that companies have "an effective compliance and ethics program" in place to prevent criminal conduct and forestall prosecution. *See* U.S. SENTENCING GUIDELINES MANUAL § 8B2.1 (U.S. SENTENCING COMM'N 2014).
292. *See supra* note 228 and accompanying text.
293. *See supra* text accompanying notes 287–89 (describing a proportionality-based data security regime).

of data security. While nonlegislative rulemaking would not provide companies with the same notice and opportunity to be heard that a notice-and-comment procedure would afford,[294] the FTC can and should solicit industry input when promulgating nonlegislative rulemaking under this Note's proposal.[295]

Next, this proposal would maximize the FTC's overarching goal of robust consumer protection. From an ex ante perspective, improved notice via nonlegislative rules would better enable companies to protect consumers before a data security breach occurs by helping them to prevent breaches in the first instance.[296] Moreover, this proposal affords the added benefit of providing nuanced guidance to companies based on the relative sensitivity of the consumer information that they retain.[297] Ex post, the FTC could continue to bring enforcement actions under section 5 against companies that fail to meet the FTC's minimum data security requirements[298] because such companies could not take advantage of the proposal's safe harbor provision.[299]

Finally, this Note's proposal, as against the proposals discussed above,[300] would provide the FTC with maximal administrative flexibility. Legislative rulemaking and congressional legislation involve many procedural obstacles, and they can be quite expensive in terms of time and money.[301] Moreover, promulgating policy through administrative adjudication provides little guidance ex ante.[302] Conversely, nonlegislative rulemaking would enable the FTC to promulgate policy ex ante, thereby providing improved guidance to regulated companies.[303] Additionally, whenever the FTC would need to change its data security policy in light of evolving technology, it would have the ability to amend any existing data security policy by issuing a new interpretive rule or policy statement.[304]

In sum, the proposal outlined in this Note, which encourages the FTC to outline minimum data security requirements that reflect the principle of

---

294. *See supra* note 202 and accompanying text (describing the benefits of legislative rulemaking).

295. Indeed, the FTC hosted a "PrivacyCon" in early 2016 where the FTC, along with stakeholders such as industry insiders, "discuss[ed] the latest research and trends related to consumer privacy and data security." *See PrivacyCon*, FED. TRADE COMM'N, https://www.ftc.gov/news-events/events-calendar/2016/01/privacycon (last visited Mar. 27, 2016) [https://perma.cc/5WQQ-PKFK]. Such events provide the FTC with an ideal opportunity to engage with industry insiders in an effort to garner input regarding data security best practices.

296. *See supra* note 228 and accompanying text.

297. *See supra* notes 287–89 and accompanying text.

298. *See supra* Part II.B.

299. *See supra* notes 290–92 and accompanying text.

300. *See supra* Part III.A.

301. *See supra* Part III.B.2–4 (discussing the shortcomings attendant to congressional legislation and legislative rulemaking).

302. *See supra* Part III.B.1 (criticizing the FTC's current ad hoc approach).

303. *See supra* notes 258–61 and accompanying text.

304. *Cf.* Perez v. Mortg. Bankers Ass'n, 135 S. Ct. 1199, 1203 (2015) (holding that agencies need not engage in legislative rulemaking to issue a new interpretation of a regulation that was originally interpreted via nonlegislative rulemaking).

proportionality via nonlegislative rulemaking,[305] would maximize the FTC's interests in providing robust consumer protection while retaining administrative flexibility.[306] In addition, the proposal goes further by ensuring that regulated companies receive ex ante guidance as to the FTC's minimum data security requirements.[307]

B. Possible Concerns Regarding Judicial Deference

In closing, Part IV.B of this Note considers one potential drawback to the novel proposal laid out in Part IV.A: the possibility of decreased judicial deference. Absent a congressional mandate to the contrary, courts typically give significant deference to an agency's interpretation of a statute that it administers.[308] However, the U.S. Supreme Court has added the caveat that an agency interpretation is only entitled to significant deference "when it appears that Congress delegated authority to the agency generally to make rules carrying the force of law, and that the agency interpretation claiming deference was promulgated in the exercise of that authority."[309] Consequently, the nonlegislative rulemaking that this Note proposes likely would receive considerably less judicial deference as against legislative rulemaking.

Notably, decreased judicial deference could put the FTC at a disadvantage if the application of its unfairness authority pursuant to this Note's proposal were challenged in court. However, the Supreme Court has also held that, given the experience and expertise of agencies like the FTC, even nonlegislative rules can garner at least some judicial deference.[310] Moreover, a reduction in judicial deference does not suggest that a given agency action is any less lawful. Thus, notwithstanding any reduced judicial deference, the FTC should not hesitate to adopt the proposal set forth in Part IV.A of this Note.

CONCLUSION

In an age where companies increasingly acquire and retain private consumer information, data security breaches are a constant threat. These breaches compromise personal information which consumers would prefer to keep private and can lead to identity theft. To combat this trend, the FTC has stepped in to prevent data security breaches by holding victimized companies accountable when their data security practices are considered inadequate. Specifically, the FTC increasingly has relied on its unfairness authority under section 5 of the FTC Act to bring enforcement actions against those companies that have not implemented "reasonable" data

305. *See supra* notes 278–92 and accompanying text.
306. *See supra* notes 236–37 and accompanying text.
307. *See supra* note 237 and accompanying text.
308. *See* Chevron, U.S.A., Inc. v. Nat. Res. Def. Council, 467 U.S. 837, 843 (1984).
309. United States v. Mead Corp., 533 U.S. 218, 226–27 (2001).
310. *See id.* at 234.

security procedures. The FTC has not, however, provided specific guidance regarding which practices it deems "unreasonable."

Although legal scholars have offered various solutions to address this lack of guidance, this Note argues that they fall short. Thus, this Note proposes a new approach. Rather than relying upon administrative adjudication, legislation, or legislative rulemaking, the FTC should engage in nonlegislative rulemaking to inform companies of its minimum data security requirements under section 5. Such rulemaking, whether in the form of an interpretive rule or policy statement, should lay out mandatory data security practices that are proportional to the consumer information that a given company retains. Furthermore, any interpretive rule or policy statement should include a safe harbor provision to ensure compliant companies that their data security practices will not be deemed "unfair." FTC implementation of this Note's proposal would ensure that: (1) companies are put on notice regarding the FTC's minimum data security requirements; (2) the FTC can continue to pursue its goal of robust consumer protection; and (3) the FTC will have maximum administrative flexibility in light of the ever-evolving technological environment that it regulates.