ESSAY

Tipping the Scales: Judicial Encouragement of a Legislative Answer to FTC Authority over Corporate Data-Security Practices

*David J. Bender**

ABSTRACT

For the first time in more than a decade of data-security enforcement actions under section 5 of the Federal Trade Commission Act, a corporation has decided to litigate the nature and extent of the Federal Trade Commission's ("FTC") authority over corporate data-security practices. Instead of agreeing to a consent decree, as most previous enforcement targets have done, Wyndham Hotel Group, LLC is challenging the very notion that the FTC may lawfully mandate specific corporate data-security practices as unfair under section 5. The Wyndham *case therefore represents the first opportunity for judicial review of the extent of the FTC's authority in this area, and the outcome will likely have far-reaching consequences in an area of law that is largely devoid of legislative direction.*

This Essay argues that the court should rule in favor of the FTC in the Wyndham litigation. Such a ruling would be consistent with Supreme Court precedents establishing that administrative agencies generally have broad discretion to choose between rulemaking and adjudication. In addition, a court

* J.D., 2013, The George Washington University Law School; B.A., 2009, Columbia University. I thank Professor Joshua I. Schwartz for his comments during the drafting of this Essay, and the editorial staff of *The George Washington Law Review* for their outstanding work. I also thank my parents and my wife Danielle for their constant support and encouragement, and my newborn daughter Samantha for napping quietly while I made the final edits.

ruling in favor of the FTC would be more likely to mobilize business interests behind legislation to specifically delineate the Agency's authority in this increasingly important area. This in turn would encourage Congress to finally heed the repeated calls of both the White House and the FTC to pass data-security legislation that would increase certainty for consumers and businesses alike.

TABLE OF CONTENTS

INTRODUCTION

On June 26, 2012, the Federal Trade Commission ("FTC" or "the Commission") filed a complaint against Wyndham Hotel Group, LLC ("Wyndham" or "Hotel Group") alleging that the company's failure to "employ reasonable and appropriate measures to protect personal information against unauthorized access" violated section 5[1] of the Federal Trade Commission Act ("FTC Act").[2] This action was nothing new for the FTC, which, since 2000, has filed forty-five (and counting) similar complaints against companies "that have violated consumers' privacy rights, or misled them by failing to maintain security for sensitive consumer information."[3] Most of these enforcement actions were settled via consent decrees, with the companies agreeing to prospectively institute more robust data-security practices.[4] Wyndham, however, chose a different route. Instead of agreeing to a settlement with the FTC, the Hotel Group litigated the issue, arguing that

---

1 First Amended Complaint for Injunctive and Other Equitable Relief at 19, FTC v. Wyndham Worldwide Corp., No. CV 12-1365-PHX-PGR (D. Ariz. Aug. 9, 2012) [hereinafter Wyndham Complaint].

2 Federal Trade Commission Act, 15 U.S.C. §§ 41–58 (2006).

3 *Legal Resources*, BUREAU OF CONSUMER PROTECTION BUS. CENTER, http://business.ftc.gov/legal-resources/29/35 (last visited July 20, 2013); *Making Sure Companies Keep Their Privacy Promises to Consumers*, FED. TRADE COMMISSION, http://www.ftc.gov/opa/reporter/privacy/privacypromises.shtml (last visited July 20, 2013).

4 *See Legal Resources*, *supra* note 3.

the FTC lacks the authority to regulate private data-security practices as "unfair" under section 5 of the FTC Act.[5] Should this case proceed, it will be the first time that a court specifically rules on the scope of the FTC's authority to regulate corporate data-security practices under the FTC Act.[6] A judicial decision in this area, where until this point the FTC has largely relied on a combination of informal guidance and consent decrees to achieve its regulatory goals,[7] could therefore significantly affect the future course of FTC regulation of data-security practices.[8]

As many others, including the FTC, have noted, the ultimate resolution of this question will have to come from Congress.[9] Given several failed attempts to date,[10] however, and the seeming inability of recent Congresses to enact large-scale legislation,[11] a legislative solution is unfortunately not likely to be forthcoming in the current environment. Furthermore, this legislative inaction is supported by the Supreme Court's rulings on the choice between rulemaking and adjudication because the Court has fostered a regime in which agencies enjoy wide discretion to choose between rulemaking and adjudication, except in certain limited circumstances.[12] Congressional inaction, combined with the Supreme Court's implicit approval of the FTC's decision to regulate via consent decrees and informal guidance, has created a status quo that is far from perfect but has been working effectively for more than a decade. Wyndham's decision to litigate the issue, however, has upset this equilibrium, and, assuming the case does not settle, the district court will need to rule one way or the

---

5 Motion to Dismiss by Defendant Wyndham Hotels & Resorts LLC at 2, FTC v. Wyndham Worldwide Corp., No. CV 12-1365-PHX-PGR (D. Ariz. Aug. 27, 2012) [hereinafter Motion to Dismiss].

6 *See* Josephine Liu, *Wyndham: FTC Lacks Authority to Regulate Data Security*, INSIDEPRIVACY (Aug. 29, 2012), http://www.insideprivacy.com/united-states/federal-trade-commission/post-on-wyndham-case/ (referring to the Wyndham case as "the first data security enforcement action to be litigated instead of being resolved by settlement").

7 *See infra* notes 68–72 and accompanying text.

8 *See* Liu, *supra* note 6.

9 *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, 171 (2008); *see also* FED. TRADE COMM'N, PRIVACY ONLINE: FAIR INFORMATION PRACTICES IN THE ELECTRONIC MARKETPLACE: A REPORT TO CONGRESS 36–37 (2000) [hereinafter 2000 FTC REPORT], *available at* http://www.ftc.gov/reports/privacy2000/privacy2000.pdf.

10 *See infra* notes 58–59 and accompanying text.

11 *See* Dana Milbank, *A House of Big Talk, No Action*, WASH. POST, May 2, 2012, at A17 ("To call this 112th Congress a do-nothing Congress would be an insult—to the real Do-Nothing Congress of 1947–48.").

12 *See infra* notes 91–97 and accompanying text.

other.[13] This Essay argues that the district court should rule in favor of the FTC by finding that the Agency has broad (though not unlimited) authority to regulate corporate data-security practices as unfair under section 5 of the FTC Act. In the current political climate, such a decision is the most likely to trigger congressional action to grant the FTC specific rulemaking authority in this area. Rulemaking authority in this increasingly important area would conserve Agency resources and at the same time provide fair warning to the regulated industry in the form of precise guidelines as to what the FTC considers unfair with respect to data-security practices.

I. THE HISTORY OF FTC REGULATION OF UNFAIR TRADE PRACTICES UNDER SECTION 5

Section 5 of the FTC Act provides that "[t]he Commission is hereby empowered and directed to prevent persons . . . from using unfair methods of competition in or affecting commerce and unfair or deceptive acts or practices in or affecting commerce."[14] This jurisdiction over "unfair" practices was first granted to the FTC in 1938,[15] but the Commission did not use the authority extensively until a 1972 Supreme Court decision encouraged the FTC to protect both consumers and competitors from unfair trade practices.[16] In *FTC v. Sperry & Hutchinson Co.*,[17] the Court approvingly quoted the Commission's criteria for unfair trade practices: "(1) whether the practice . . . offends public policy . . .; (2) whether it is immoral, unethical, oppressive, or unscrupulous; [and] (3) whether it causes substantial injury to con-

13 Settlement of the Wyndham litigation prior to a decision on the merits is unlikely. This is the first, and thus far only, data-security enforcement action to reach the motion to dismiss stage precisely because Wyndham, unlike every previous enforcement target, refused to settle with the FTC. Instead, Wyndham chose to litigate the issue, and in so doing has directly attacked the FTC's statutory authority to enforce particular data-security practices. Absent a sudden shift in FTC policy, which is unlikely given that the Commission has continued to take similar enforcement actions subsequent to the one against Wyndham, *see* Press Release, Fed. Trade Comm'n, Tracking Software Company Settles FTC Charges That It Deceived Consumers and Failed to Safeguard Sensitive Data It Collected (Oct. 22, 2012), http://ftc.gov/opa/2012/10/compete.shtm, a court will have a chance to rule on the case. Even if the parties settle, the substantive legal issue of the FTC's authority to enforce specific data-security practices will eventually be decided by a court, at which point this Essay argues that the court should rule in favor of the FTC.

14 15 U.S.C. § 45(a)(2) (2006).

15 Wheeler-Lea Amendment of 1938, Pub. L. No. 75-447, § 5(a), 52 Stat. 111, 111–12 (codified as amended at 15 U.S.C. § 45(a)(2)).

16 *See* FTC v. Sperry & Hutchinson Co., 405 U.S. 233, 244 (1972); *see also* Scott, *supra* note 9, at 135–36.

17 FTC v. Sperry & Hutchinson Co., 405 U.S. 233 (1972).

sumers."[18] *Sperry*, combined with a statute granting the FTC rulemaking authority,[19] led to an "ensuing decade of 'over-exuberance' as the agency tested the outer limits of its powers."[20]

The FTC's newfound enthusiasm for enforcing the unfairness prong of section 5 was met with substantial criticism,[21] however, and Congress responded with the 1980 Federal Trade Commission Improvements Act,[22] which severely curtailed the FTC's rulemaking authority over unfair trade practices.[23] The legislation reflected congressional concern that "in many instances the FTC had taken actions beyond the intent of Congress"[24] and sought to remedy this overreaching by prohibiting the use of the unfairness doctrine in certain industries and significantly increasing the administrative burden of unfairness doctrine rulemaking.[25] Later that same year, the Commission wrote a letter to the Senate Committee on Commerce, Science, and Transportation in which it "narrow[ed] the unfairness doctrine."[26] In the letter, the Commission admitted that "the concept of consumer unfairness is one whose precise meaning is not immediately obvious, and also recognize[d] that this uncertainty has been honestly troublesome for some businesses and some members of the legal profession."[27] The letter further noted, however, that section 5

---

18 *Id.* at 244–45 n.5 (quoting Unfair or Deceptive Advertising and Labeling of Cigarettes in Relation to the Health Hazards of Smoking, 29 Fed. Reg. 8324, 8355 (July 2, 1964)).

19 Magnuson-Moss Warranty—Federal Trade Commission Improvement Act, Pub. L. No. 93-637, 88 Stat. 2183 (1975) (codified as amended at 15 U.S.C. §§ 2301–2312 (2006)).

20 Robert A. Skitol, *How BC and BCP Can Strengthen Their Respective Policy Missions Through New Uses of Each Other's Authority*, 72 ANTITRUST L.J. 1167, 1169 (2005).

21 *See, e.g.*, S. REP. NO. 96-500, at 525–26 (1979), *reprinted in* 1980 U.S.C.C.A.N. 1102, 1103 ("In the recent past, the FTC has come under attack for embarking upon rulemaking proceedings which have aroused considerable criticism."); Editorial, *The FTC as National Nanny*, WASH. POST, Mar. 1, 1978, at A22 (referring to the FTC as the "national nanny" after the Commission attempted to ban all advertising directed at children).

22 *See* Federal Trade Commission Improvements Act of 1980, Pub. L. No. 96-252, 94 Stat. 374 (codified as amended in scattered sections of 15 U.S.C.).

23 *Id.* (prohibiting use of the unfairness doctrine in several specified proceedings and curtailing its use in rulemaking).

24 S. REP. NO. 96-500, at 526.

25 *See* Federal Trade Commission Improvements Act of 1980, 94 Stat. at 374; *see also infra* notes 37–39 and accompanying text.

26 Ernest Gellhorn, *Trading Stamps, S&H, and the FTC's Unfairness Doctrine*, 1983 DUKE L.J. 903, 956.

27 Letter from Michael Pertschuk et al, Chairman & Comm'rs, Fed. Trade Comm'n, to Wendell H. Ford, Chairman, and John C. Danforth, Ranking Minority Member, Consumer Subcomm. of the Senate Comm. on Commerce, Sci., & Transp. (Dec. 17, 1980), *reprinted in* Int'l Harvester Co., 104 F.T.C. 949, 1071 (1984).

> was deliberately framed in general terms since Congress recognized the impossibility of drafting a complete list of unfair trade practices that would not quickly become outdated or leave loopholes for easy evasion. The task of identifying unfair trade practices was therefore assigned to the Commission, subject to judicial review, in the expectation that the underlying criteria would evolve and develop over time.[28]

Finally, the FTC agreed to abandon the second element quoted in *Sperry*, whether the practice is unethical or unscrupulous,[29] and "pledged to proceed only if either the unjustified consumer injury test or the violation of public policy test was satisfied."[30]

The FTC formally adopted the principles from the letter in a policy statement as the agency standard for unfair trade practices in 1984,[31] and Congress codified a version of the Agency's definition of unfairness in the 1994 amendments to the FTC Act.[32] Under this test, an unfair trade practice is one which (1) causes or is likely to cause substantial injury to consumers; (2) is not reasonably avoidable by consumers; and (3) is "not outweighed by countervailing benefits to consumers or to competition."[33] Moreover, the FTC "may consider established public policies" to determine whether an act or practice is unfair, but may not use them as the "primary basis" for that determination.[34] The FTC has the authority to enjoin unfair trade practices by filing suit in federal district court,[35] as the Commission has done in the *Wyndham* case.[36]

---

28 104 F.T.C. at 1072 (footnote omitted).

29 FTC v. Sperry & Hutchinson Co., 405 U.S. 233, 244 n.5 (1972).

30 Gellhorn, *supra* note 26, at 942; *see also* 104 F.T.C. at 1076 ("The Commission has therefore never relied on the [unethical or unscrupulous conduct element] as an independent basis for a finding of unfairness, and it will act in the future only on the basis of the first two.").

31 *See* 104 F.T.C. at 1076.

32 Federal Trade Commission Act Amendments of 1994, Pub. L. No. 103-312, sec. 9, § 5(n), 108 Stat. 1691, 1695 (codified at 15 U.S.C. § 45(n) (2006)). Section 5(n) provides that:

> The Commission shall have no authority under this section or section 18 to declare unlawful an act or practice on the grounds that such act or practice is unfair unless the act or practice causes or is likely to cause substantial injury to consumers which is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition. In determining whether an act or practice is unfair, the Commission may consider established public policies as evidence to be considered with all other evidence. Such public policy considerations may not serve as a primary basis for such determination.

15 U.S.C. § 45(n) (2006).

33 *Id.*

34 *Id.*

35 *See* 15 U.S.C. § 53(b) (2006).

36 *See* Wyndham Complaint, *supra* note 1.

In addition to this enforcement authority, the FTC may prescribe "rules which define with specificity acts or practices which are unfair."[37] This rulemaking authority, however, is significantly more burdensome than standard agency rulemaking under the Administrative Procedure Act ("APA").[38] For instance, in addition to the standard APA requirements, the FTC is required to publish "with particularity the text of the [proposed] rule, including any alternatives,"[39] and also provide an opportunity for an informal hearing where interested parties may cross-examine witnesses.[40] Therefore, although the FTC technically has rulemaking authority to define specific unfair practices, Congress has effectively stripped the Agency of any practical ability to make data-security rules absent specific authorization.[41] In this environment, it is not surprising that the Commission has thus far not published any rules or regulations defining specific data-security policies as unfair trade practices under the FTC Act.[42] The Commission itself has acknowledged the impracticability of rulemaking absent specific statutory authorization, noting in congressional testimony that a provision in a bill allowing it to use standard notice and comment rulemaking would allow it "to promulgate these rules in a more timely and efficient manner."[43]

Congressional codification of the FTC's unfairness standard coincided with the beginning of the rapid growth of the internet, particularly as an online marketplace.[44] Since that time, the Commission has

---

37 15 U.S.C. § 57a(a)(1)(B).

38 Administrative Procedure Act, 5 U.S.C. §§ 551–559, 701–706 (2006); *see id.* § 553.

39 15 U.S.C. § 57a(b)(1).

40 *Id.* § 57a(c).

41 Recognizing the impracticability of general rulemaking authority under the FTC Act, Congress has granted the FTC rulemaking authority over data-security practices in certain limited contexts. *See, e.g.*, Fair Credit Reporting Act, 15 U.S.C. § 1681m(e) (rulemaking for financial institutions to reduce the incidence of identity theft); Children's Online Privacy Protection Act, 15 U.S.C. § 6502(b)(1) (rulemaking authority to protect the confidentiality and security of information obtained from children).

42 *See* Scott, *supra* note 9, at 144 (noting "the lack of any rulemaking proceedings, policy statements or guidelines from the Commission explaining what conduct" constitutes an unfair trade practice in the realm of data security); *see also* Motion to Dismiss, *supra* note 5, at 3 ("The FTC has not published *any* rules or regulations that might provide the business community with *ex ante* notice of what data-security protections a company must employ to be in compliance with the law.").

43 *Discussion Draft of H.R. ___, A Bill to Require Greater Protection for Sensitive Consumer Data and Timely Notification in Case of Breach: Hearing Before the Subcomm. on Commerce, Mfg., & Trade of the H. Comm. on Energy & Commerce*, 112th Cong. 11 (2011) (statement of Edith Ramirez, Comm'r, Federal Trade Commission), *available at* http://www.ftc.gov/os/testimony/110615datasecurityhouse.pdf.

44 *See* 2000 FTC REPORT, *supra* note 9, at 1 ("[From 1995–2000], the Internet has changed

taken an active role in shaping online privacy and data-security policy.[45] Based on the results of a survey of online privacy in 2000, the Commission noted the broad scope of online data collection:

> Web sites collect a vast amount of personal information from and about consumers. This information is routinely collected from consumers through registration forms, order forms, surveys, contests, and other means, and includes personal identifying information, which can be used to locate or identify an individual, and non-identifying information. The Commission's Survey findings demonstrate that nearly all Web sites collect personal identifying information from consumers.[46]

Initially, the FTC promoted industry self-regulation to address consumers' increased concern about the privacy of their online data.[47] In a 2000 report to Congress (the "2000 FTC Report"), however, the Commission noted that the "limited success of self-regulatory efforts to date make it time for government to act to protect consumers' privacy on the Internet."[48] Self-regulation was inadequate to meet the "enormous public policy challenge" of online privacy,[49] so the FTC "recommend[ed] that Congress enact legislation" that "would set out the basic standards of practice governing the collection of information online, and provide an implementing agency with the authority to promulgate more detailed standards pursuant to the Administrative Procedure Act, including authority to enforce those standards."[50] Finally, in a statement that would later be used against it in the Wyndham litigation,[51] the Commission explained that such congressional action was necessary because "the Commission lacks authority to require firms to adopt information practice policies or to abide by the fair information practice principles on their Web sites."[52]

Since the 2000 FTC Report, the scope of online commerce and attendant consumer privacy concerns has only grown in scale and im-

---

dramatically from a large network of computers that touched the lives of few consumers to a new marketplace where millions of consumers shop for information, purchase goods and services, and participate in discussions.").

45 *Id.* at 3.

46 *Id.* at 9 (footnotes omitted).

47 *Id.* at 2; *see also id.* at 3 ("[The Commission] has continued to encourage and facilitate effective self-regulation to protect consumers generally.").

48 *Id.* at 36.

49 *Id.* at ii.

50 *Id.* at 36 (footnote omitted).

51 *See infra* Part III.

52 2000 FTC REPORT, *supra* note 9, at 34.

portance.[53] As more and more companies collect data about their customers, the vulnerability of that data to security breaches has come to the forefront.[54] Responding to these growing concerns, the White House joined the FTC in calling for congressional action on baseline privacy legislation.[55] Despite the exhortations of the Commission and the White House, Congress still has yet to provide the FTC with specific rulemaking authority over online privacy and data security.[56] Although several currently pending bills would give the FTC rulemaking authority to establish guidelines for data-security breach notification, none of them grant the Commission the power to enforce specific data-security policies or establish guidelines that it might apply in enforcement actions against companies with inadequate data security.[57] A number of these bills have been pending for years, and none of them have gone further than the committee reporting stage.[58] In fact, Congress seems unable to pass anything other than symbolic privacy legislation—the only privacy-related bills passed in the preceding two years have been identical resolutions "expressing support for the designation of January 28 . . . as 'National Data Privacy Day.'"[59] The White House itself seems skeptical that Congress will grant the FTC

---

53 *See* Edward Wyatt, *F.T.C. and White House Push for Online Privacy Laws*, N.Y. TIMES, May 10, 2012, at B8 ("Privacy concerns have come to the fore as consumers grow increasingly aware of just how closely their actions online are tracked.").

54 *See id.*

55 *See* WHITE HOUSE, CONSUMER DATA PRIVACY IN A NETWORKED WORLD: A FRAMEWORK FOR PROTECTING PRIVACY AND PROMOTING INNOVATION IN THE GLOBAL DIGITAL ECONOMY 36 (2012) [hereinafter 2012 WHITE HOUSE REPORT] ("The Administration encourages Congress to follow a similar path with baseline consumer data privacy legislation.").

56 *See* Scott, *supra* note 9, at 143 ("Over seven years have passed since the Commission pushed for specific legislation to provide broad consumer privacy protection, but Congress thus far has declined to act."); *see also* FED. TRADE COMM'N, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE: RECOMMENDATIONS FOR BUSINESSES AND POLICYMAKERS 12–13 (2012) [hereinafter 2012 FTC REPORT], *available at* http://www.ftc.gov/os/2012/03/120326privacyreport.pdf (noting, in March of 2012, that "in addition to reiterating its call for federal data security legislation, the Commission calls on Congress to consider enacting baseline privacy legislation" (footnote omitted)).

57 *See* Scott, *supra* note 9, at 173 ("However, none of these bills currently address the FTC's jurisdiction to take action against entities that experience data security breaches, or the rules the Commission should apply in determining when to take such action.").

58 *See, e.g.*, Data Security and Breach Notification Act of 2012, S. 3333, 112th Cong. (2012) (as referred to committee on June 21, 2012); Personal Data Privacy and Security Act of 2011, S. 1151, 112th Cong. (2011) (as reported by committee on Sept. 22, 2011); Personal Data Protection and Breach Accountability Act of 2011, S. 1535, 112th Cong. (2011) (as reported by committee on Sept. 22, 2011). Earlier versions of each of these bills "remain[ed] pending in Congress" as of 2008. Scott, *supra* note 9, at 172.

59 S. Res. 358, 112th Cong. (2012) (enacted on Jan. 30, 2012); S. Res. 35, 112th Cong. (2012) (enacted on Jan. 31, 2011).

rulemaking and enforcement power over data security anytime in the near future.[60] Given the current political climate, the chances that Congress will fill the legislative void in data-security regulation and enforcement are quite slim, at least without significant prodding.

II. FTC ENFORCEMENT OF INADEQUATE CORPORATE DATA SECURITY AS AN UNFAIR TRADE PRACTICE

Understandably frustrated with the lack of a legislative solution, the FTC has taken matters into its own hands by challenging inadequate corporate data-security practices as unfair trade practices under section 5. Although the Commission arguably disclaimed this authority in the 2000 FTC Report,[61] it soon changed course after Timothy Muris became FTC Chairman in 2001 and indicated that the Commission would pursue aggressive enforcement of consumer protection laws.[62] The Commission began using its section 5 authority to pursue websites for a variety of deceptive acts or practices.[63] Additionally, starting in 2005, the FTC began pursuing companies for data-security breaches as unfair under section 5, even if those companies did not engage in any deceptive practices.[64] This shift by the Commission was not coincidental, as 2005 has been referred to as "The Year of the Data Breach," when "media outlets were flooded with stories of one data breach after another."[65] In the first such case, the FTC filed a complaint against BJ's Wholesale Club ("BJ's") alleging unfair trade practices for the company's failure to ensure "reasonable security" for its network after hackers downloaded customer bank card information to make fraudulent purchases.[66] In what would soon become a pattern, BJ's quickly agreed to a consent order, lasting for twenty years, in which it agreed to institute various data-security practices.[67]

---

60 *See* 2012 WHITE HOUSE REPORT, *supra* note 55, at 2 ("*Even if Congress does not pass legislation*, the Consumer Privacy Bill of Rights will serve as a template for privacy protections that increase consumer trust on the Internet and promote innovation." (emphasis added)).

61 *See supra* note 52 and accompanying text.

62 *See* Scott, *supra* note 9, at 131.

63 *See id.* at 133–34; *see also infra* note 68 and accompanying text.

64 *See* 2012 FTC REPORT, *supra* note 56, at A-5; *see also* Scott, *supra* note 9, at 145–46.

65 John P. Hutchins & Renard C. Francois, *A New Frontier: Litigation Over Data Breaches*, PRAC. LITIGATOR, July 2009, at 47, 47.

66 *See* Scott, *supra* note 9, at 146.

67 *See id.* at 147. Among other requirements, the BJ's consent order requires the company to designate "an employee or employees to coordinate and be accountable for the information security program," identify "material internal and external risks to . . . security," and design and implement "reasonable safeguards to control the risks identified through risk assessment, and regular testing." BJ's Wholesale Club, Inc., 140 F.T.C. 465, 471 (2005).

The FTC has continued this practice with other companies, each time negotiating a nearly identical twenty-year consent order mandating specific data-security practices.[68] Generally, these consent orders require the companies to submit periodic independent audit results and other reports indicating compliance with the Commission's data-security standards.[69] Unsurprisingly, practitioners carefully monitor these consent orders and use them as de facto data-security law in the absence of specific regulations.[70] The FTC appears to encourage this practice, and has at least implied that companies should consider the string of consent orders to represent what the Commission considers adequate data-security practices.[71] For instance, FTC Chairman Jon Leibowitz recently testified that "[t]he Commission's robust enforcement actions have sent a strong signal to industry about the importance of data security, while providing guidance about how to accomplish this goal."[72]

Nevertheless, the FTC's enforcement of data-security policies under the unfairness prong of the FTC Act has been met with substantial criticism. These critiques generally relate to three basic problems with the Commission's strategy. First, commentators have criticized the Commission for effectively rulemaking through adjudication, which does not provide fair notice to similarly situated parties

---

68 *See, e.g.*, Decision and Order at 6–7, UPromise, Inc., No. C-4351 (F.T.C. Mar. 27, 2012), *available at* http://www.ftc.gov/os/caselist/1023116/120403upromisedo.pdf (nearly identical terms to the BJ's order); Decision and Order at 3, Premier Capital Lending, Inc., No. C-4241 (F.T.C. Dec. 10, 2008), *available at* http://www.ftc.gov/os/caselist/0723004/081216pcldo.pdf (same); Decision and Order at 3, CardSystems Solutions, Inc., No. C-4168 (F.T.C. Sept. 5, 2006), *available at* http://www.ftc.gov/os/caselist/0523148/0523148CardSystemsdo.pdf (same).

69 *See, e.g.*, Consent Decree and Order for Civil Penalties, Injunction, and Other Relief at 11, United States v. RockYou, Inc., No. 12-CV-1487 (N.D. Cal. Mar. 27, 2012), *available at* http://ftc.gov/os/caselist/1023120/120327rockyouorder.pdf.

70 *See* David Alan Zetoony, *The 10 Year Anniversary of the FTC's Data Security Program: Has the Commission Finally Gotten Too Big for Its Breaches?*, STAN. TECH. L. REV., at ¶ 8 (Dec. 27, 2011), http://stlr.stanford.edu/pdf/zetoony-ten-year-anniversary.pdf ("In the absence of case law, the legal community has used these consent orders as evidence of the types of practices that the Commission believes violate the law, and as a benchmark for the type of relief that would be available to the Commission if it were to proceed to trial against a company that is alleged to have provided inadequate security.").

71 *See* Statement of Julie Brill, Comm'r, Fed. Trade Comm'n, in Which Chairman Leibowitz and Commissioners Rosch and Ramirez Join, In the Matters of SettlementOne Credit Corporation, ACRAnet, Inc., and Fajilan and Associates, (revised Aug. 15, 2011), *available at* http://www.ftc.gov/os/2011/08/110819settlementonestatement.pdf.

72 *Consumer Online Privacy: Hearing Before the S. Comm. on Commerce, Sci., & Transp.*, 111th Cong. 11 (2010) (statement of Jonathan D. Leibowitz, Chairman, Federal Trade Commission).

as to precisely what conduct is prohibited.[73] Second, commentators have noted that the absence of what the Commission considers to be adequate data-security policies does not constitute an unfair trade practice under the Commission's own definition of unfairness.[74] Third, from a policy standpoint, these data breaches are perpetrated by hackers rather than the companies themselves, and the Commission should focus its efforts on going after the hackers rather than their corporate victims.[75] Assuming the Wyndham case does not settle prior to a court ruling, the district court will have the opportunity to address each of these arguments. When it does so, the court should rule in favor of the FTC because, when properly analyzed, none of these points foreclose FTC regulation of corporate data-security practices through adjudication.

III. THE WYNDHAM LITIGATION: HOW THE COURTS CAN FACILITATE A REAL SOLUTION TO CORPORATE DATA-SECURITY REGULATION

The Wyndham case presents the first opportunity for a court to decide whether the FTC can enforce data-security practices under the unfairness prong of section 5 of the FTC Act. In an area where the law has largely been made through informal guidance and consent decrees, a judicial decision one way or the other will have significant ramifications. If the district court rules in favor of Wyndham, the Commission's ability to regulate corporate data-security practices as unfair under the FTC Act will be sharply restricted. Until Congress passes legislation, corporate data-security practices will largely be dictated by self-regulation, a regime that the Commission has demonstrated is wholly inadequate to achieving the goal of consumer protection in data security.[76] If, however, the district court rules in favor of the Commission, the FTC can continue to enforce corporate data-security practices moving forward until Congress finally acts, which it will be more likely to do in the first place.

---

73 *See, e.g.*, Hutchins & Francois, *supra* note 65, at 50 ("In its actions under the FTC Act against entities experiencing data breaches, the FTC has likewise relied on fear and shame—the fear that large, high-profile business [sic] have of being 'the test case' under Section 5, and the shame associated with a large-scale data breach, principally the desire for the story simply to go away.").

74 *See, e.g.*, Zetoony, *supra* note 70, at ¶ 39 ("It is highly doubtful that the practice about which the Commission complains—a failure to police a company's customers by monitoring their data security practices—meets any of [the FTC's unfairness] criteria.").

75 *See id.* at ¶¶ 9–10.

76 *See supra* notes 47–48 and accompanying text.

This Essay argues that the district court should rule in the FTC's favor. Such a decision would be consistent with Supreme Court precedents affirming federal agencies' broad discretion to choose between rulemaking and adjudication except in specific circumstances, and would also incentivize Congress to act quickly and grant the Commission rulemaking authority over this increasingly important area. In the end, therefore, a decision in favor of the FTC would be a net positive for both sides. Consumers would continue to enjoy the benefits of aggressive FTC enforcement of robust corporate data security. Meanwhile, businesses would benefit from increased certainty about the bounds of FTC authority under the FTC Act, as well as the increased likelihood of congressional legislation to further define what constitutes unfair trade practices with regard to data security.

The arguments made by Wyndham largely track the recurrent themes that commentators have advanced in response to FTC enforcement of data-security practices through adjudication.[77] Wyndham argues that nothing in the text or legislative history of the FTC Act grants the Commission the authority to regulate data security, and that the agency specifically disclaimed that authority.[78] Citing *FDA v. Brown & Williamson Tobacco Corp.*,[79] Wyndham argues that the FTC is exercising its authority here in a manner that is inconsistent with the statutory scheme, and that Congress would not delegate a decision of such magnitude in so cryptic a fashion as "unfair trade practices" in section 5.[80] Moreover, even if the FTC Act does grant the Commission authority to regulate data security, Wyndham argues that such data-security standards must be enforced "ex ante through rulemaking, rather than ex post through a selective enforcement action."[81] Wyndham cites *Ford Motor Co. v. FTC*[82] and *NLRB v. Bell Aerospace Co.*[83] for the proposition that "when an agency tries to use an adjudication to announce new principles of law that could have widespread application, the agency has abused its authority."[84] Finally, Wyndham applies the FTC's unfairness test to the facts of the case and argues that the injuries from data-security breaches are avoidable and not

77 *See supra* notes 73–75 and accompanying text.

78 *See* Motion to Dismiss, *supra* note 5, at 6–7.

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

80 *See* Motion to Dismiss, *supra* note 5, at 6, 8–9 (citing *Brown & Williamson*, 529 U.S. at 125, 160).

81 *Id.* at 10.

82 Ford Motor Co. v. FTC, 673 F.2d 1008 (9th Cir. 1981).

83 NLRB v. Bell Aerospace Co., 416 U.S. 267 (1974).

84 Motion to Dismiss, *supra* note 5, at 10–11.

substantial, and therefore are not unfair trade practices under the FTC Act.[85]

Representing "the nation's business community,"[86] the Chamber of Commerce, among others, filed an amicus curiae brief urging the court to dismiss the case against Wyndham.[87] Referring to the Commission's expansive use of its unfairness authority in the 1970s prior to congressional limitations,[88] the amici argued that the "FTC has strayed down the same path again."[89] In addition, the amici advanced many of the same arguments as Wyndham: that the FTC lacks authority to regulate data security and that the Commission's "backdoor rulemaking" without congressional action is impermissible.[90]

Although Wyndham and others have argued that the FTC has impermissibly engaged in adjudication in an area where it should have used rulemaking, agencies generally maintain wide discretion to choose between the two devices except in specific circumstances.[91] The circumstances in which an agency cannot use adjudication in lieu of rulemaking include: (1) when the agency lacks authority to use adjudication at all;[92] (2) creation of a binding statement of law or policy that only applies prospectively;[93] (3) direct reversal of prior precedent relied upon by the parties with an accompanying retrospective sanction;[94] (4) narrowing of the scope of an entitlement;[95] (5) disregard of a regulation that is still in effect;[96] or (6) when the use of adjudication

---

85 *See id.* at 12–14.

86 Brief for Chamber of Commerce of the United States of America et al. as Amici Curiae Supporting Defendants at 1, FTC v. Wyndham Worldwide Corp., No. CV 12-1365-PHX PGR (D. Ariz. Oct. 5, 2012) [hereinafter Amici Brief].

87 *Id.* at 15.

88 *See supra* notes 15–20 and accompanying text.

89 Amici Brief, supra note 86, at 2.

90 *Id.* at 13.

91 *See* NLRB v. Bell Aerospace Co., 416 U.S. 267, 294 (1974) (broad agency discretion to choose between rulemaking and adjudication); SEC v. Chenery Corp., 332 U.S. 194, 203 (1947) ("And the choice made between proceeding by general rule or by individual, ad hoc litigation is one that lies primarily in the informed discretion of the administrative agency.").

92 *See* Nat'l Petroleum Refiners Ass'n v. FTC, 482 F.2d 672, 674 (D.C. Cir. 1973) (FTC could not engage in rulemaking absent statutory authority).

93 *See* NLRB v. Wyman-Gordon Co., 394 U.S. 759, 772–75 (1969) (Black, J., concurring).

94 *See Bell Aerospace*, 416 U.S. at 294 (stating in dictum that direct reversal of prior precedent relied upon by parties which imposes retrospective sanction may be an abuse of discretion). Wyndham's reliance on *Bell Aerospace* is misplaced because the Court specifically held that the agency did not abuse its discretion by announcing new principles in an adjudication. *See id.*

95 *See* Morton v. Ruiz, 415 U.S. 199, 231–32 (1974).

96 *See* United States *ex rel.* Accardi v. Shaughnessy, 347 U.S. 260, 266–67 (1954); *see also* Leslie v. Attorney Gen., 611 F.3d 171, 175–76 (3d Cir. 2010) (referring to the doctrine that agencies must follow their own rules as "the *Accardi* doctrine").

is a flagrant abuse of discretion.[97] None of these situations are present in the Wyndham case. The FTC has authority to use adjudication under the FTC Act.[98] This enforcement action does not make binding statements of law that apply only prospectively or directly reverse prior precedent because it seeks only prospective injunctive relief,[99] and it is consistent with previous enforcement actions.[100] The FTC is not narrowing the scope of any entitlement in these cases, nor is it disregarding any regulation in bringing them. Finally, although many have argued that the Agency's action here overreaches and that rulemaking would be preferable to decide this recurring issue, the use of adjudication here is hardly a flagrant abuse of discretion, especially because, as a practical matter, the Commission lacks effective rulemaking authority here.[101] In fact, *Bell Aerospace*[102] and *SEC v. Chenery Corp.*[103] indicate that adjudication is permissible even when not preferable.[104] Therefore, the Wyndham court should rule that it was not an abuse of discretion for the FTC to choose adjudication in this instance.

Although the FTC, the White House, and Congress all agree that legislation is necessary in this context, and that rulemaking would be preferable to adjudication, the court in Wyndham must nevertheless decide the case before it. Some have argued that courts should rule in a way that facilitates a deliberative process,[105] which in this case would mean ruling in a way that is most likely to encourage congressional legislation in this area. In the Wyndham case, the ruling most likely to

---

97 *See* Ford Motor Co. v. FTC, 673 F.2d 1008, 1010 (9th Cir. 1981) (requiring the FTC to use rulemaking rather than adjudication when the regulated party had "[n]o notice" of the FTC's novel interpretation of state law). Wyndham's reliance on *Ford Motor* is misplaced because it reads the decision too broadly to prohibit announcement of general principles via adjudication. *See* Motion to Dismiss, *supra* note 5, at 11. Nothing in *Ford Motor*, however, changes the principle that agencies enjoy wide discretion to choose between rulemaking and adjudication, absent the type of flagrant abuse of discretion at issue in that case.

98 *See* 15 U.S.C. § 53(b) (2006).

99 Wyndham Complaint, *supra* note 2, at 20.

100 *See supra* notes 66–68 and accompanying text.

101 *See supra* note 41 and accompanying text. While the D.C. Circuit held that the FTC had substantive rulemaking authority to regulate business conduct, that decision was in 1973, before Congress severely limited the Commission's rulemaking authority in 1980. *See* Nat'l Petroleum Refiners Ass'n v. FTC, 482 F.2d 672, 674 (D.C. Cir. 1973); *see also supra* notes 21–25 and accompanying text.

102 NLRB v. Bell Aerospace Co., 416 U.S. 267 (1974).

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

104 *See id.* at 202; *Bell Aerospace*, 416 U.S. at 294.

105 *See* WILLIAM N. ESKRIDGE, JR., PHILIP P. FRICKEY & ELIZABETH GARRETT, CASES AND MATERIALS ON LEGISLATION 409–10, 428 (4th ed. 2007) (describing the theory of due process of lawmaking that courts should act to encourage legislative deliberation).

prompt congressional action is a ruling in favor of the FTC that the Commission *does* have the authority to regulate data-security practices under the FTC Act and that Wyndham's actions fall under the definition of unfair trade practices.[106] This is because business interests are against the Commission in this case,[107] and a ruling against these business interests would lead to increased pressure on Congress to act and define the boundaries of FTC authority to regulate data security. Moreover, industry interest groups are well organized in opposition to data-security legislation, which would have distributed benefits for consumers and concentrated costs for industry.[108] Congress has yet to weigh in on the current regulatory environment, where the FTC relies on consent decrees on uncertain legal footing.[109] This status quo cannot continue, however, as Wyndham has challenged the basis of the FTC's enforcement authority over data security.[110] Although Congress might well agree with Wyndham and legislate to curtail the FTC's authority over data security, that would at least provide consumers, industry, and the FTC itself clear notice of the bounds of FTC authority in the area. The FTC and the White House are already strongly behind data-security legislation,[111] such that a court decision against the FTC would not likely increase the pressure on Congress to legislate. A decision in favor of the FTC, however, and against industry interests, is most likely to encourage legislative deliberation because it would mobilize industry interests that currently appear largely satisfied with the status quo.[112]

As the FTC's opposition to the motion to dismiss illustrates, the court could rule in the Commission's favor on firm legal grounds, despite several commentators' prediction that a court would likely rule

---

106 In ruling on the Motion to Dismiss, of course, the court would not reach the merits and decide whether Wyndham's actions are unfair, which is a "fact-specific inquiry and, thus, inappropriate for a motion to dismiss." Plaintiff's Response in Opposition to Wyndham Hotels and Resorts' Motion to Dismiss at 14, FTC v. Wyndham Worldwide Corp., No. 2:12-cv-01365-PHX-PGR (D. Ariz. Oct. 1, 2012) [hereinafter FTC Wyndham Response]. However, the court should rule that the FTC has pled sufficient facts to survive the motion to dismiss, allowing the case to proceed to the merits.

107 *See* Amici Brief, *supra* note 86, at 1, 3.

108 *See* ESKRIDGE, *supra* note 105, at 57 ("Opposition will tend to be well organized" to legislation with distributed benefits and concentrated costs).

109 *See supra* notes 68–70 and accompanying text.

110 *See supra* note 78 and accompanying text.

111 *See supra* note 55 and accompanying text.

112 Prior to *Wyndham* each of the similar enforcement actions ended in consent decrees, illustrating industry willingness to go along with the status quo. *See supra* note 4 and accompanying text.

against the FTC.[113] Even if the Commission previously disclaimed the authority to regulate data security, which the FTC disputes,[114] agencies are free to change positions, particularly when the alleged previous position was merely a policy statement rather than a formal rule or adjudication.[115] Additionally, although Wyndham argues that data-security regulation does not appear in the text of section 5,[116] the FTC nevertheless retains the ability to regulate data security that is in or affecting commerce, as "[s]ection 5 does not identify specific acts or practices."[117] Section 5 is written in broad terms precisely because one cannot anticipate changes in technology that might call for new applications of the unfair trade practice principles. Unlike in *Brown & Williamson*, where the FDA's interpretation "plainly contradict[ed] congressional policy,"[118] the presence of specific data-security statutes regarding certain industries does not preclude coverage of data security more generally under the FTC Act because those industry-specific statutes grant the Commission legal tools beyond those in the FTC Act.[119] Furthermore, unlike *Brown & Williamson*, where the regulation of tobacco was well established when the relevant statute was enacted,[120] no one could have imagined the modern data-security context in 1938, when section 5 was enacted. In deciding that Congress expressed clear intent to preclude FDA jurisdiction over tobacco products, the *Brown & Williamson* Court relied on Congress' clear intent to preclude such jurisdiction, evidenced by legislation that created a distinct regulatory scheme to address the tobacco problem.[121] In contrast, Congress could not have had a "clear intent"[122] with regard to data security when section 5 was enacted because the concept did not even exist at the time.

---

113 *See, e.g.*, Hutchins & Francois, *supra* note 65, at 48; Zetoony, *supra* note 70, at ¶ 44 ("[T]he Commission may have difficulty defending its jurisprudence-by-acclamation in court.").

114 *See* FTC Wyndham Response, *supra* note 106, at 7–8.

115 *See* Chevron U.S.A., Inc. v. Natural Res. Def. Council, Inc., 467 U.S. 837, 863–64 (1984) (EPA was allowed to change its interpretation of the word "source" because it had a rational basis for doing so and "[a]n initial agency interpretation is not instantly carved in stone").

116 Motion to Dismiss, *supra* note 5, at 6.

117 FTC Wyndham Response, *supra* note 106, at 6.

118 FDA v. Brown & Williamson Tobacco Corp., 529 U.S. 120, 139 (2000).

119 *See* FTC Wyndham Response, *supra* note 106, at 8. For example, the Fair Credit Reporting Act and Children's Online Privacy Protection Act grant the FTC authority to impose civil penalties for certain unreasonable data-security practices. *See* 15 U.S.C. § 1681 (2006); 15 U.S.C. §§ 6501–6506 (2006).

120 *Brown & Williamson*, 529 U.S. at 125–26.

121 *Id.* at 143–44.

122 *Id.* at 126.

With respect to Wyndham's argument about the lack of express congressional authorization, as is often the case, the significance of congressional debate and inaction to this point can be argued either way. Although Wyndham argues that the intense debate in Congress over data security makes it unlikely that the Commission already has authority to regulate it under the FTC Act,[123] the FTC responds that "[i]f relevant at all, the facts of the congressional debate over data security affirm" the Commission's interpretation due to the longstanding agency practice and failure of Congress to limit the agency's actions.[124]

Turning to the elements of an unfairness violation under 15 U.S.C. § 45(n), the FTC has alleged that "[c]onsumers and businesses suffered financial injury, including, but not limited to, unreimbursed fraudulent charges, increased costs, and lost access to funds or credit."[125] Assuming these allegations are established at trial, and Wyndham's data-security policies led to breaches which caused "the known theft of hundreds of thousands of consumers' payment card account numbers, and millions of dollars in fraud loss,"[126] this would be more than enough to meet the substantial injury, not reasonably avoidable by consumers, and countervailing benefit balancing requirements. Finally, although Wyndham is likely correct that the hackers are more morally culpable than the corporations in these cases, enforcement actions against individual hackers are neither practical nor cost-effective.[127] Therefore, from a policy standpoint, focusing agency resources against inadequate corporate data-security policies is strongly preferable to enforcement actions against individual hackers, who are difficult to locate and likely judgment-proof.

CONCLUSION

The Wyndham litigation presents the first judicial opportunity to decide whether the FTC has the authority to regulate data security through targeted enforcement actions that effectively set a minimum standard for corporate data-security practices. Although it is true that such generally applicable standards are more properly the subject of

123 Motion to Dismiss, *supra* note 5, at 8–9.

124 FTC Wyndham Response, *supra* note 106, at 10.

125 Wyndham Complaint, *supra* note 2, at 18.

126 FTC Wyndham Response, *supra* note 106, at 1.

127 *See* Michael Lee et al., Comment, *Electronic Commerce, Hackers, and the Search for Legitimacy: A Regulatory Proposal*, 14 BERKELEY TECH. L.J. 839, 875 (1999) ("[H]ackers are generally judgment-proof, so victims of hacking intrusions are usually left without financial remedy . . . ." (footnote omitted)).

rulemaking than adjudication, rulemaking is not practically achievable until Congress acts to grant the FTC standard APA rulemaking authority over data-security practices. And the best way to encourage Congress to legislate, in an area where it has failed to do so for more than a decade despite repeated requests and attempts, is for a court to rule in a way that is most likely to force Congress's hand. Therefore, the court in Wyndham should rule in favor of the FTC, thus mobilizing business interests squarely behind congressional action, which is already supported by the executive branch and the agency itself. Wyndham has upset an equilibrium in which the FTC has been effectively enforcing data-security policies through repeated adjudications, and instead of foreclosing the agency's ability to do so until Congress acts (if it ever does), the court should take this as an opportunity to tip the scales in favor of a legislative solution.