Fight or Comply: The Federal Trade Commission's Power to Hold Companies Liable for Data Security Breaches

Sarah Sargent*

I. INTRODUCTION

Verizon's 2014 Data Breach Investigations Report named 2013 "the year of the

* I would like to thank my family and friends for supporting me throughout my academic experience. I would also like to thank Matt Neumann and the Volume 40 *Journal of Corporations Law* editors for working with me on the piece and providing valuable feedback during its construction. Finally, I would like to thank my professors at the University of Iowa College of Law for providing a supportive and challenging learning environment. You all have aided in my endeavors, and I am forever thankful.

retailer breach."[1] In July, Harbor Freight, an American tool vendor, reported the largest retailer breach ever.[2] The breach affected over 445 stores and 200 million customers.[3] Retailers, however, were not the only companies to fall victim to data breaches. CNN, the Washington Post, Time Magazine, the New York Post, and the New York Times were all targets of cyber-espionage in 2013.[4] One possible explanation for the increased level of data security breaches is criminals becoming more technology savvy, but the Verizon report concluded that despite the high levels of breaches in 2013, nine basic hacking patterns account for 95% of all breaches.[5] Therefore, the problem lies within the business networks rather than in an increase of criminal sophistication.

The Federal Trade Commission (FTC) reacted to large-scale, highly publicized data breaches by filing complaints against businesses lacking data security protections to prevent breaches.[6] The FTC's recent actions resulted in companies and scholars questioning the FTC's jurisdictional authority and inquiring about the constitutionality of the agency's actions regarding data security.[7] The primary issue stems from the vague standard to which the FTC holds companies.[8] This Note addresses why the FTC possesses the authority to regulate data security under the FTC Act, examines the legal standard to which companies are held, and advises companies on how to act in the current regulatory atmosphere. Part II describes the operational basis of the FTC and provides a history of the agency's involvement with data security regulation, including recent litigation. Part III explains recent court decisions and analyzes their effect on current regulation. Part IV is two-fold. First, Section IV.A addresses why the recent court decisions were correct in upholding FTC authority over data security regulation. Second, Section IV.B recommends businesses comply with current regulation by following FTC settlements and industry developed best practices while lobbying for clarification of the FTC's expectations of data security.

II. BACKGROUND: HOW THE FTC BEGAN REGULATING DATA SECURITY POLICIES THROUGH SECTION 5

This Part will review the current framework of the FTC. The framework includes specific statutory provisions as well as FTC-established policy. Additionally, a brief history of the FTC's involvement with data security then provides background for the current legal fights surrounding the FTC's jurisdiction.

A. Statutory Framework: The Federal Trade Commission Act

The FTC Act empowers the FTC under section 5 to prevent companies "from using

1. VERIZON, 2014 DATA BREACH INVESTIGATIONS REPORT 3 (2014), https://www.cisco.com/web/strategy/docs/retail/verizon_2014_breachreport.pdf.
2. *Id.*
3. *Id.*
4. *Id.*
5. *Id.*
6. *See infra* Section II.E (discussing FTC v. Wyndham Worldwide Corp., 10 F. Supp. 3d 602 (D.N.J. 2014)).
7. *Infra* Section III.B.
8. *See infra* Section III.B.3 (explaining how companies are left without a definition of the reasonable data security practices standard due to the lack of formalized FTC rules and adjudicated FTC cases).

unfair methods of competition in or affecting commerce and unfair or deceptive acts or practices in or affecting commerce."[9] Under the authority of the FTC Act, the FTC regulates data security using deceptive practice claims and unfair practice claims.[10] Companies engage in deceptive practices when they violate their own data privacy policies.[11] In a deceptive practices claim, the FTC must show the company made a material representation that would mislead reasonably acting consumers.[12] The FTC holds broad discretion to determine what constitutes an unfair practice.[13] The FTC must ensure the unfair practice "causes or is likely to cause substantial injury to consumers which is not reasonably avoided by consumers themselves"[14] and is "not outweighed by countervailing benefits to consumers or to competition."[15] When the FTC files complaints against companies for unfair practices involving data securities, the FTC utilizes a standard of reasonableness and determines whether the company's data security systems "reasonably" protect consumers from substantial harm.[16]

The FTC also holds the power to issue rules to specifically define what unfair practices are. However, the FTC Act requires Magnuson-Moss rulemaking, a more extensive rulemaking process than the typical Administrative Procedure Act requirements.[17] Magnuson-Moss rulemaking requires the FTC to engage in extensive public hearings, which include evidence and opportunities for rebuttal, before adopting a proposed rule.[18] Magnuson-Moss rulemaking also requires FTC rules to be reviewed under a higher, substantial evidence standard.[19] Due to the extra statutory requirements, the FTC has not developed specific rules governing unfair practices involving data security practices.[20]

Along with the FTC Act, other federal statutes regulate data security in specific industries.[21] For example, the Gramm-Leach-Bliley Act regulates financial institutions,

---

9. 15 U.S.C. § 45 (2012).

10. Peter S. Frechette, FTC v. LabMD*: Jurisdiction Over Information Privacy Is "Plausible," But How Far Can It Go?*, 62 AM. U.L. REV. 1401, 1403 (2013).

11. *Id.*

12. *Id.* at 1404.

13. Congress purposely defined "unfair practices" generally in order to give the FTC power to maintain regulation that was up to speed with technology and current business practices. *See* David J. Bender, *Tipping the Scales: Judicial Encouragement of a Legislative Answer to FTC Authority Over Corporate Data-Security Practices*, 81 GEO. WASH. L. REV. 1665, 1669 (2013) (discussing the content of a letter the FTC wrote to a senate committee discussing its power regarding unfair trade practices); *see also* Elie Freedman, *An Era of Rapid Change: The Abdication of Cash & the FTC's Unfairness Authority*, 14 U. PITT. J. TECH. L. & POL'Y 351, 356 (2014) (discussing the decision in *FTC v. Sperry & Hutchinson Co.* which states Congress explicitly granted the FTC the power to define unfair practices).

14. 15 U.S.C. § 45 (2012).

15. *Id.*

16. Frechette, *supra* note 10, at 1405.

17. Standard agency rulemaking is governed by 5 U.S.C. § 553 (2012). Bender, *supra* note 13, at 1671. The FTC's rulemaking authority under the statute is often referred to as Magnuson-Moss rulemaking. Gerard M. Stegmaier & Wendell Bartnick, *Psychics, Russian Roulette, and Data Security: The FTC's Hidden Data-Security Requirements*, 20 GEO. MASON L. REV. 673, 692 (2013).

18. FED. TRADE COMM'N, OPERATING MANUAL ch. 7, 3–5 (1990), http://www.ftc.gov/sites/default/files/attachments/ftc-administrative-staff-manuals/ch07rulemaking.pdf (listing the required steps in FTC rulemaking).

19. Hybrid Rulemaking Procedures of the FTC, 44 Fed. Reg. 38817 (July 3, 1979).

20. Stegmaier & Bartnick, *supra* note 17, at 674 (discussing the lack of specific data security practice rules).

21. *See* Corey M. Dennis & David A. Goldman, *Data Security Laws and the Cybersecurity Debate*, 17 J. INTERNET L. 1, 10 (2013) (listing federal data security laws, including the Health Information Technology for

and the Fair Credit Reporting Act regulates consumer protection agencies.[22] State laws also address the issue of data security by requiring companies to act reasonably in order to safeguard consumer data.[23] Most state laws require companies to take certain steps when data breaches occur.[24] However, there are multiple approaches for when a company must notify customers.[25]

B. Soft Law: The FTC's Development of Reports and Guidelines

Reports and guidelines provide the majority of information regarding the FTC's policies and expectations in data security practices.[26] These reports and guidelines are "soft law," meaning the agency creates the policies through informal means.[27] In May 2012, the FTC issued a report titled, *Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers*.[28] The report included a number of recommendations, such as incorporating substantive privacy protections, limiting data collection, notifying customers of privacy policy breaches, and taking steps to ensure the company is meeting consumer expectations.[29] FTC reports rely primarily on the Fair Information Practice Principles (FIPPs), which hold companies to the reasonableness standard.[30] Published guidelines, such as *Protecting Personal Information: A Guide for Business*, also recommend specific data security practices.[31] The guideline recommends certain training for employees, updating firewalls, limiting employee access to data, encrypting files, and other specific actions.[32] Despite the FTC taking the time and money to publish a substantial amount of recommendations and guidelines, the FTC never articulated whether the recommendations are mandatory.[33]

C. Transition from Self-Regulation to Active Regulation

Originally, the FTC relied on a system of company self-regulation under the FTC Act.[34] Companies would establish their own standards by adopting privacy policies, and the FTC would police companies by using deceptive practice claims based on the

---

Economic and Clinical Health Act and the Children's Online Privacy Protection Act).

22. Dana Rosenfeld & Donnelly McDowell, *Moving Target: Protecting against Data Breaches Now and Down the Road*, 28 ANTITRUST 90, 90 (2014).

23. *Id.* at 91.

24. *Id.* at 92 (stating 46 state laws contain breach notification requirements which require companies to notify customers of any breach of personal information).

25. *Id.*

26. Daniel J. Solove & Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, 114 COLUM. L. REV. 583, 626 (2014).

27. *Id.*

28. Freedman, *supra* note 13, at 365.

29. *Id.* at 365–66. The report identified five action items which included: "(1) Do-Not-Track; (2) mobile security and privacy; (3) transparency in data brokerage; (4) security of 'large platforms' . . . (5) further development of self-regulatory codes." Frechette, *supra* note 10, at 1408.

30. Frechette, *supra* note 10, at 1406.

31. Stegmaier & Bartnick, *supra* note 17, at 694.

32. FED. TRADE COMM'N, PROTECTING PERSONAL INFORMATION: A GUIDE FOR BUSINESS (Nov. 2011), https://www.ftc.gov/system/files/documents/plain-language/bus69-protecting-personal-information-guide-business_0.pdf.

33. Solove & Hartzog, *supra* note 26, at 626.

34. Frechette, *supra* note 10, at 1410–11.

companies' own policies.[35] The FTC first started to question the self-regulatory scheme in the *2000 FTC Report*, which claimed self-regulation was "inadequate to meet the 'enormous public policy challenge' of online privacy."[36] After the FTC issued the report, both the FTC and the White House requested Congress pass legislation specifically addressing the FTC's authority over data security practices; however, Congress was unable to pass any legislation.[37]

In 2001, a new FTC Chairman, Timothy Muris, implemented a policy to aggressively enforce consumer protection laws by pursuing companies for data security breaches under unfair practice claims.[38] After multiple large-scale data security breaches became public, the FTC also began pursuing companies solely under unfair practice claims even when the company did not engage in deceptive practices.[39] The FTC first filed a complaint against BJ's Wholesale Club for unfair trade practices when the company failed to prevent hackers from downloading customer credit card information.[40] The FTC filed a complaint after it became known hackers were able to steal the credit card information of thousands of customers due to BJ's poor network security.[41] The FTC filed a complaint against BJ's because the store:

> (1) did not encrypt the information while in transit or when stored on the in-store computer networks; (2) stored the information in files that could be accessed anonymously—that is, using a commonly known default user id and password; (3) did not use readily available security measures to limit access to its computer networks through wireless access points on the networks; (4) failed to employ sufficient measures to detect unauthorized access or conduct security investigations; and (5) created unnecessary risks to the information . . . .[42]

In 2008, the FTC issued the *2008 Resolution* establishing the Commission's investigatory authority over businesses engaged in deceptive or unfair practices relating to consumer privacy and data security.[43] In 2010, the FTC began using a harm-based model in applying unfair or deceptive practice claims, which targeted practices that caused economic harm to consumers.[44] Since 2000, the number of privacy related claims has increased each year.[45] Despite the increased number of claims, the FTC remains very selective in which claims it brings due to limited agency resources.[46] The FTC has brought over 170 claims against companies related to data privacy; however, only three claims resulted in judicial action.[47] The first case, *FTC v. Accusearch, Inc.*, ended with the Tenth

35. *Id.* at 1411.
36. Bender, *supra* note 13, at 1672.
37. *Id.* at 1673. Congress has still not been able to pass any legislation regarding the FTC's authority in regards to data security practices. *Id.*
38. *Id.* at 1674.
39. *Id.*
40. Bender, *supra* note 13, at 1674.
41. BJ's Wholesale Club, Inc., 140 F.T.C. 465, 476 (2005).
42. *Id.*
43. Freedman, *supra* note 13, at 362.
44. Frechette, *supra* note 10, at 1407.
45. Solove & Hartzog, *supra* note 26, at 600.
46. *See id.* at 624 (quoting a former associate director from the FTC about the claim strategy of the agency).
47. *Id.* at 611.

Circuit upholding the broad authority of the FTC.[48] The other two cases, *In re LabMD, Inc.* and *FTC v. Wyndham Worldwide Corp.*, both involve unfair practice complaints and are currently in litigation.[49] Part II discusses both cases further in depth.[50]

The majority of claims end in settlement with a consent order[51] imposing the adoption of specific data security practices and mandatory inspections and reports from the consenting business.[52] Consent orders typically last 20 years, but the time can be shorter or longer (even indefinite).[53] Usually, consent orders include prohibitions on wrongful activity, fines and other monetary penalties, consumer notification and remediation requirements, deleting data, making changes in privacy policy, establishing comprehensive programs, assessments by independent professionals, record keeping, compliance reports, and notification of material changes affecting compliance.[54] The FTC uses consent orders to informally notify other companies when a certain practice is prohibited.[55] Before the FTC accepts a consent order, it publishes the order and accepts comments from third-parties.[56] Once the FTC accepts the order, the FTC sends letters answering the concerns of any commentators.[57] The vast majority of companies settle due to the costs of litigation, the low civil penalties, the unlikelihood of winning in adjudication, and the avoidance of reputational costs.[58]

D. Recent FTC Data Security Regulation: LabMD, Inc. v. FTC

LabMD, Inc. v. FTC is one of three cases that did not settle after receiving a FTC complaint. The FTC brought an unfair practices claim against LabMD for failing to reasonably protect patient information on its internal network.[59] LabMD attempted to quash the FTC's Civil Investigative Demand (CID) ordering the company to turn over information.[60] LabMD argued, "the FTC's claim of authority to regulate data security 'is not based on any threat of substantial injury to consumers, but only generalities.'"[61] The court did not accept LabMD's argument and instead upheld the statutory authority and jurisdiction of the FTC to regulate data security.[62] After the court order requiring LabMD to comply with the CID, the FTC completed its investigation and continued agency adjudication.[63]

---

48. *Id.* at 611 n.121 ("[T]he FTCA enables the FTC to take action against unfair practices that have not yet been contemplated by more specific laws." (citing FTC v. Accusearch Inc., 570 F.3d 1187, 1193–95 (10th Cir. 2009))).

49. *Infra* Section II.D–E.

50. *Id.*

51. *See* Solove & Hartzog, *supra* note 26, at 611–12 (discussing why most data security claims end in settlement consent orders).

52. Bender, *supra* note 13, at 1675.

53. Solove & Hartzog, *supra* note 26, at 614.

54. *Id.* at 614–19.

55. *Id.* at 622.

56. *Id.* at 623.

57. *Id.*

58. Solove & Hartzog, *supra* note 26, at 611–14.

59. LabMD, Inc. v. FTC, No. 1:14–cv–00810–WSD, 2014 WL 1908716, at *1 (N.D. Ga. May 12, 2014).

60. Frechette, *supra* note 10, at 1409–10.

61. Freedman, *supra* note 13, at 364.

62. *Id.*

63. *See LabMD, Inc., In the Matter of*, FED. TRADE COMM'N, https://www.ftc.gov/enforcement/cases-

E. FTC Holding Companies Liable for Third-Party Data Breaches: FTC v. Wyndham

FTC v. Wyndham Worldwide Corp. was the first case in which the FTC filed a complaint for unfair and deceptive business practices due to a third-party data security breach.[64] The FTC filed a complaint against Wyndham after the company failed to reasonably protect customers' data information.[65] Russian hackers accessed Wyndham's network three separate times using the same method and entry point into the company's network.[66] The three data breaches compromised more than 619,000 customers and cost $10.6 million in fraudulent charges.[67] Wyndham sought to have the complaint dismissed on the grounds that "(1) the FTC lacks authority to pursue unfair practices related to data-security, (2) the unfairness action related to data security requires rulemaking, and (3) the injury resulting from these payment card breaches is insufficient to support a claim."[68] In response, the FTC argued Congress purposefully granted the Commission broad powers to determine what unfair practices encompass, rulemaking in data security practices is impractical, and the injury to consumers was not fully mitigated through reimbursement.[69] The court agreed and upheld the FTC's broad authority under the FTC Act.[70]

III. ANALYSIS: EXPLAINING THE COURTS' DECISIONS TO UPHOLD FTC JURISDICTION OVER DATA SECURITY POLICIES AND THE CONSEQUENCES

This Part first discusses recent court decisions upholding FTC power in order to address why the current regulatory scheme remains problematic. Next, Part III presents two differing scholarly opinions analyzing the issues created by FTC regulations. Finally, Part III explains and examines the consequences of the recent court decisions.

A. The Courts' Reasoning Behind Backing FTC Authority

1. LabMD, Inc. v. FTC

The *LabMD* court upheld the FTC's jurisdiction to regulate data security practices under section 5 of the FTC Act based largely upon precedent[71] that recognizes the FTC's power to define unfair practices.[72] The court further explained because of the high rate of exploitation inherent in data security breaches, the injury qualified as a substantial harm to

---

proceedings/102-3099/labmd-inc-matter (last updated Sept. 14, 2015) (listing the current status of the agency adjudication).

64. Freedman, *supra* note 13, at 367.

65. FTC v. Wyndham Worldwide Corp., 10 F. Supp. 3d 602, 607 (D.N.J. 2014).

66. *Id.* at 608.

67. *Id.* at 609.

68. Freedman, *supra* note 13, at 372.

69. *Id.* at 375–77.

70. *Id.* at 377.

71. "Congress has not at any time withdrawn the broad discretionary authority originally granted to the Commission in 1914 to define unfair practices on a flexible, incremental basis. Courts have accordingly adopted a malleable view of the Commission's authority." Am. Fin. Servs. Ass'n v. FTC, 767 F.2d 957, 967–68 (D.C. Cir. 1985) (citing FTC v. Sperry & Hutchinson Co., 405 U.S. 233, 244 (1972), Atlantic Refining Co. v. FTC, 381 U.S. 357, 367 (1965)).

72. Frechette, *supra* note 10, at 1412 (citing FTC v. LabMD, Inc., No. 1:12-cv-3005, slip op. at 13 (N.D. Ga. Nov. 26, 2012)).

consumers, which granted the FTC jurisdiction.[73] While the court did confirm the FTC's jurisdiction over data security practices, it only addressed jurisdiction relating to investigatory action.[74] When reviewing an agency's investigatory action, courts only ask whether there is a "plausible argument" for jurisdiction.[75] The court, therefore, neither fully addressed the broad jurisdictional power of the FTC nor applied any due process analysis to determine whether the FTC was providing fair notice of its regulatory expectations.

2. FTC v. Wyndham*: The Ground Breaking Path*

The district court in *Wyndham* addressed three issues about the FTC's unfairness claim.[76] First, the court addressed Wyndham's claim that the FTC did not have authority under section 5 to regulate data security practices pursuant to the decision in *Brown & Williamson*.[77] The court found *Brown & Williamson* did not apply to data security practices because Congress did not create a distinct regulatory scheme for data security regulation as it did with the tobacco industry.[78] Instead, the court found the regulatory schemes governing specific industries' data security co-exist with the FTC's jurisdiction.[79] Since the *Brown & Williamson* exception did not preclude the FTC's authority, the court did not further address the issue.

Second, the court addressed whether the fair notice doctrine requires the FTC to publish formal rules and regulations prior to enforcement.[80] The court cited well established precedent that states when an agency is "given an option to proceed by rulemaking or by individual adjudication the choice is one that lies in the informed discretion of the administrative agency."[81] In fact, the court noted, "the Circuit Courts of Appeal have affirmed FTC unfairness actions in a variety of contexts *without* preexisting rules or regulations."[82] The court stated the FTC does not need to issue specific regulations in order to give fair notice to companies about what specifically violates section 5 data security standards.[83] In support of this conclusion, the court listed several other agencies that regulate without particularized prohibitions.[84] The court further indicated a lower court

73. *Id.* at 1412–13.

74. *Id.* at 1413.

75. *Id.*

76. FTC v. Wyndham Worldwide Corp., 10 F. Supp. 3d 602, 612–26 (D.N.J. 2014).

77. *Id.* at 612. In *Brown & Williamson*, the Supreme Court held the FDA did not have authority to regulate the tobacco industry because Congress had implemented legislation which specifically regulated the tobacco industry, meaning Congress intended for the industry-specific legislation to regulate. FDA v. Brown & Williamson Tobacco Corp., 529 U.S. 120, 161 (2000).

78. *Wyndham*, 10 F. Supp. 3d at 612–13.

79. *Id.* at 613.

80. *Id.* at 616.

81. *Id.* at 617 (citing PBW Stock Exch., Inc. v. SEC, 485 F.2d 718, 732 (3d Cir. 1973)).

82. *Id.* at 618.

83. *See Wyndham*, 10 F. Supp. 3d at 620–21 (noting precedent suggesting the FTC need not publish formal rules since section 5 is necessarily flexible).

84. *Id.* at 620 (giving examples of when the National Labor Relations Board, the Occupational Safety and Health Administration, and the Department of Homeland Security do not use particularized prohibitions in enforcement).

would not find section 5 to be vague under a Rule 12(b)(6)[85] motion.[86]

The third issue the district court decided was whether the injury was substantial and satisfied section 5 requirements.[87] The court found all of the section 5 requirements of an unfair practice to be met because an injury can be substantial "if it does a small harm to a large number of people."[88] The court noted the standard of review for a motion to dismiss requires a favorable inference be drawn for the plaintiff.[89]

The court ultimately attempted to narrow its holding by stating "[i]nstead, the [c]ourt denies a motion to dismiss given the allegations in *this* compliant—which must be taken as trust *at this stage*—in view of binding and persuasive precedent."[90] The court's opinion indicated the great weight and importance of precedence that confirms the FTC's discretionary powers under the vague language of section 5. Even though the order represents the initial stages of litigation, the court's decision not to dismiss recognizes how lenient courts are when reviewing agency decisions. Given that the trial court will use the same precedent and principles in its final ruling, it is likely the court will ultimately uphold the FTC's authority.[91]

Once the district court ruled in favor of the FTC, the Third Circuit granted interlocutory appeal on two issues: (1) whether the FTC possessed authority under the unfairness prong of section 5 to regulate data security; and (2) whether Wyndham had fair notice of the FTC's regulation of data security.[92] Wyndham argued, for the first time on appeal, the FTC could only regulate unfair practices if the practice "injure[d] consumers 'through unscrupulous or unethical behavior.'"[93] The Third Circuit rejected Wyndham's argument stating the Supreme Court already ruled unfair practices need not be unethical or scrupulous.[94] Wyndham also argued if the court ruled in favor of the FTC, the FTC would possess infinite power to regulate all aspects of business including the posting of guards at hotel room doors.[95] The court dismissed the argument as "alarmist at the least" and held Wyndham's behavior could fall within the meaning of unfair conduct.[96] Wyndham next renewed its argument from the district court level stating the FTC was precluded from regulating data security under *Brown & Williamson*.[97] The Third Circuit affirmed the district court's ruling that recent legislation did not preclude the FTC from regulating data security because the legislation required rather than authorized the FTC to regulate.[98]

Second, Wyndham argued the company did not receive fair notice as required by the due process clause because the FTC did not declare unreasonable data security practices as

85. FED. R. CIV. P. 12(b)(6).
86. *Wyndham*, 10 F. Supp. 3d at 621.
87. *Id.* at 623.
88. *Id.* (citing Am. Fin. Servs. Ass'n v. FTC, 767 F.2d 957, 972 (D.C. Cir. 1985)).
89. Freedman, *supra* note 13, at 379.
90. *Wyndham*, 10 F. Supp. 3d at 610.
91. *See* Freedman, *supra* note 13, at 381 (arguing the court will most likely continue to uphold the FTC's jurisdiction over data security issues in the trial stage of *Wyndham*).
92. FTC v. Wyndham Worldwide Corp., No 14-3514, 2015 WL 4998121, at *1 (3d Cir. Aug. 24, 2015).
93. *Id.* at *5.
94. *Id.*
95. *Id.* at *7.
96. *Id.*
97. *Wyndham*, 2015 WL 4998121, at *7.
98. *Id.* at *8.

unfair.[99] While Wyndham argued they were entitled to notice with ascertainable certainty of the FTC's interpretation of data securities requirements, the court held Wyndham was only entitled to fair notice of what conduct could fall under the meaning of section 5.[100] The level of notice required depends on the context of the circumstances.[101] The court explained Wyndham was entitled to a low level of notice because of the civil and economic nature of section 5.[102] The court held section 5 is not so vague as to not provide a legal rule or standard at all.[103] Due to Wyndham's multiple breaches and complete lack of security measures, the court stated Wyndham should have known its behavior possibly fell within the regulated category.[104] In analyzing the fair notice claim, the court considered the FTC's consent order, complaints, and guidelines.[105]

B. Consequences of LabMD *and* Wyndham

1. Consequences: The FTC's Authority to Move Forward in Data Security Regulation

As the FTC continues to move forward in data security regulation, two opposing viewpoints have emerged on what the future holds for the FTC's authority. On one side, legal scholars argue the FTC's soft law guidelines do not provide sufficient fair notice to withstand a constitutional challenge.[106] Scholars argue the FTC has not given constitutionally required fair notice because the agency has not published rules or rule proceedings in the federal register, has only used informal adjudication in accepting consent orders, and has not published policy statements that specifically address its interpretation of section 5 in data security practices.[107] The opposing viewpoint argues the soft law guidelines and consent orders have formed a valid common law, which does provide fair notice.[108] While the Third Circuit upheld the FTC's regulation under a fair notice analysis, another court will likely not address the issue until *LabMD* finishes its litigation.[109]

The most frequent criticism of the current FTC data security soft law is the FTC has provided neither formally published rules nor formally adjudicated decisions.[110] The FTC explains the reasonableness standard to which it holds companies works better with rules

99. *Id.* at *12.

100. *Id.* at *13.

101. *Id.* at *9.

102. *Wyndham*, 2015 WL 4998121, at *13 (stating economic regulation statutes "receive a 'less strict' test because their 'subject matter is often more narrow, and because businesses, which face economic demands to plan their behavior carefully, can be expected to consult legislative regulation in advance").

103. *Id.*

104. *Id.* at *14.

105. *Id.* at *15.

106. Stegmaier & Bartnick, *supra* note 17, at 720. *See also* Bender, *supra* note 13, at 1675–76 (stating critics believe rules must be either published or determined by adjudication in order to meet fair notice requirements); Gerard M. Stegmaier & Wendell Bartnick, *Another Round in the Chamber: FTC Data Security Requirements and the Fair Notice Doctrine*, 17 J. INTERNET L. 1, 26–27 (2013) (claiming the agency's publications of its data security policy would not satisfy the fair notice requirements of the D.C. Circuit Court).

107. Stegmaier & Bartnick, *supra* note 17, at 699–701.

108. Solove & Hartzog, *supra* note 26, at 619.

109. *See* LabMD, Inc. v. FTC, 776 F.3d 1275, 1280 (11th Cir. 2015) (stating the district court has no jurisdiction to review LabMD's claims of unconstitutionality until a final agency decision is reached).

110. Stegmaier & Bartnick, *supra* note 106, at 26.

formed through adjudication rather than formal rulemaking because of the nature of data security regulations.[111] The problem then stems from the lack of adjudicated data security practice cases. However, with almost all of the complaints ending in settlement agreements prior to adjudication, case law is not established to provide direction for companies.[112] The final litigation in *LabMD* and *Wyndham* could very well provide the adjudicated rules critics call for, but companies will have to wait for the lengthy litigation process to end.

Scholars draw a distinction between the soft law (guidelines and reports) and the consent orders when analyzing constitutional fair notice issues.[113] Specifically, they argue settlements have a greater weight and enforceability than guidelines or reports, which only indicate how the FTC might regulate in a specific case.[114] While the privacy settlements "technically lack precedential force for other companies," advising counsels utilize the consent orders as adjudicated precedent.[115] In fact, before the FTC accepts the consent order, the FTC publishes it in the federal register for notice and comment similar to a formal rule.[116] Some practitioners believe consent orders have more of an impact than specific litigation.[117] Internal procedures of the FTC indicate the agency itself treats consent orders as a method of creating enforcement standards.[118] In fact, the FTC strategically aims to bring cases that will cause a large impact on other businesses to conserve agency resources.[119] Scholars recommend lawyers treat the consent orders as a body of common law because the orders provide predictability as to how the FTC will enforce section 5.[120]

2. Future Implications: Will Congress Listen?

Scholars who believe the FTC lacks legislative authority under section 5 to pursue data security regulation hope the final *Wyndham* court's decision to uphold the FTC will result in congressional action.[121] The FTC called on Congress before to pass legislation confirming its ability to regulate data security law;[122] however, Congress has yet to pass any legislation mainly due to its fundamental disagreement over which cyber security problems to address and which government institution would be best suited to address them.[123] Critics believe a decision favoring the FTC's broad power will incite industry leaders to take a more active role in persuading Congress to pass legislation limiting FTC authority over data security practices.[124] Additionally, practitioners believe the court's backing of the FTC will likely result in the expansion of regulation surrounding data

111. FTC v. Wyndham Worldwide Corp., 10 F. Supp. 3d 602, 620 (D.N.J. 2014).
112. Bender, *supra* note 13, at 1675–76.
113. Solove & Hartzog, *supra* note 26, at 626.
114. *Id.*
115. *Id.* at 620.
116. *Id.* at 621.
117. *Id.*
118. Solove & Hartzog, *supra* note 26, at 623 (stating the agency will use previous consent orders in drafting new pleadings).
119. *Id.* at 624.
120. *Id.* at 625.
121. Bender, *supra* note 13, at 1677.
122. Frechette, *supra* note 10, at 1415.
123. Jorge L. Contreras et al., *Mapping Today's Cybersecurity Landscape*, 62 AM. U. L. REV. 1113, 1119–20 (2013).
124. Bender, *supra* note 13, at 1680.

security practices.[125] In fact, the FTC has recently brought complaints against Credit Karma and Fandango relating to the company's mobile applications.[126]

3. No Single Standard: What Is Reasonable and How Do Businesses Conform?

While scholars debate the constitutional principles of the FTC's data security regulation, businesses are left without a discernible standard to follow. All businesses know is that their data security practices must be reasonable, but they are left without adjudicated precedent or formal rules to indicate what a reasonable standard entails.[127] Unless Congress lowers the standard for FTC formal rulemaking from Magnuson-Moss rulemaking[128] to regular APA rulemaking procedure,[129] the FTC will most likely not even consider adopting formal rules indicating what suffices as reasonable.[130] Businesses could just wait to see if adjudication produces rules. However, if businesses do not attempt to ascertain what the FTC expects now, they could be opening themselves up to future liability.[131]

The lack of a standard is one reason that practitioners recommend companies turn to the consent orders for clarification on the reasonableness standard.[132] The issue with using consent orders as the primary indicator of FTC policy is each consent order is specific to the company on which it is imposed; therefore, the listed data security practice could protect one company while leaving another vulnerable.[133] Additionally, consent orders use vague phrases, such as "reasonably designed to . . . address security risks related to the development and management of new and existing covered devices."[134]

In fact, the FTC guidelines specifically state, "[t]here [is] no one-size-fits-all approach to data security, and what [is] right for you depends on the nature of your business and the kind of information you collect from your customers."[135] Therefore, even if companies treat consent orders and guidelines as rules, there is no guarantee of avoiding a future complaint by the FTC. Given that the Federal Bureau of Investigation states there are two categories of companies, "those that have been hacked, and those that will be,"[136] the likelihood a company will at some point deal with a data security breach, and therefore deal with the FTC, is too great for a company to chance liability because they wrongly

125. *See* Rosenfeld & McDowell, *supra* note 22, at 93 (arguing enforcement agencies will draw upon existing authority in order to start new initiatives in data security issues).

126. *Id.* at 92.

127. Stegmaier & Bartnick, *supra* note 17, at 704.

128. 15 U.S.C. §§ 2310(a)(1–2), 2311(b)(c) (2012).

129. 5 U.S.C. § 553 (2012).

130. *See* Stegmaier & Bartnick, *supra* note 17, at 692 (explaining the additional requirements imposed on Magnuson-Moss rulemaking such as extra informal hearings with oral testimony).

131. *See id.* at 720 (stating that the aggressive enforcement of the FTC requires businesses to perform proper risk management which requires interpreting the FTC's section 5 power).

132. Solove & Hartzog, *supra* note 26, at 621–22 (discussing a number of lawyers and firms which recommend clients follow consent orders in order to determine what the FTC is regulating).

133. *See* Stegmaier & Bartnick, *supra* note 17, at 717 (stating it is unclear whether nonparties should follow consent orders because the FTC does not list specific details about the types of data being regulated).

134. HTC Am., Inc., Docket No. C-4406 (June 25, 2013), http://www.ftc.gov/sites/default/files/documents /cases/2013/07/130702htcdo.pdf.

135. *See* Stegmaier & Bartnick, *supra* note 17, at 718 (discussing the lack of clarity in terms used in guidelines).

136. Frechette, *supra* note 10, at 1402.

ascertained the meaning of "reasonable."

VI. RECOMMENDATIONS: COMPANIES SHOULD ATTEMPT TO DISCERN REASONABLENESS, ADOPT SIMILAR POLICIES ACCORDINGLY, AVOID COSTLY LITIGATION, AND LOBBY

This Note's recommendation is two-fold. First, it addresses the steps companies should take to avoid an FTC complaint. Second, it addresses what other actions companies should take to address the legal ambiguities the law created. The recommendations are based on the high likelihood the courts will continue to uphold FTC jurisdiction and authority to regulate data security.

A. How to Discern Reasonableness: What Data Security Businesses Should Adopt Now

Since businesses are currently left without a clear standard for reasonable data security practices,[137] businesses must weigh the costs and benefits of adopting the data security standards recommended in soft law and consent orders. However, many businesses struggle with the cost-benefit analysis for adopting particular data security practices because of the constantly changing technology and business-specific requirements.[138] A recent survey of CEOs revealed two-thirds of businesses do not believe they have enough information to accurately translate information technology risk into business risk.[139] Some attorneys who follow the guidelines and settlements of the FTC recommend at least adopting monitoring systems for reasonably foreseeable vulnerabilities, developing network perimeter controls such as firewalls and limited device access, encrypting data, and limiting access to networks through usernames and complex passwords.[140] Other attorneys state changing the network alone is not sufficient and businesses should also create a culture of data security through training employees, creating committees to analyze issues, and developing strategies in case a breach occurs.[141] Even if businesses take steps to have reasonable data security practices, however, technology causes industry standards—and therefore FTC standards—to change rapidly, which opens up businesses to regulatory liability.[142]

Additionally, companies could look to non-government sources to discern what is reasonable. One source companies could look to for guidance on standard industry practice is the International Organization for Standardization (ISO). The ISO is an independent, non-governmental membership organization that establishes international standards of

137. *See supra* Section III.C (discussing how the FTC has not adopted rules or adjudicated cases in order to establish a meaning of reasonable data security practices).

138. Contreras et al., *supra* note 123, at 1121 (analyzing the work of Michael McNerney, a former Cyber Policy Advisor in the Office of the Secretary of State, who discussed the difficulties in assessing the value of cybersecurity and costs of security failures). The FTC guidelines state "[t]here's no one-size-fits-all approach to data security, and what's right for you depends on the nature of your business and the kind of information you collect." Stegmaier & Bartnick, *supra* note 17, at 718.

139. Michael McNerney & Emilian Papadopoulos, *Hacker's Delight: Law Firm Risk and Liability in the Cyber Age*, 62 AM. U. L. REV. 1243, 1266 (2013).

140. Bret Cohen, *The Law of Securing Consumer Data on Networked Computers*, 18 J. INTERNET L. 3, 5–9 (2014).

141. McNerney & Papadopoulos, *supra* note 139, at 1265–68.

142. *See* Cohen, *supra* note 140, at 9 (discussing the ever-changing FTC standards and their consequences).

practice in various industries.[143] The ISO creates standards through technical committees that help develop industry standards for a particular field.[144] In fact, the ISO's technical committee for information technology developed a standard catalog of information technology security techniques, which is accessible for free on the internet.[145] The catalog includes documents describing standards for entity authorization, digital signature checks, evaluation criteria for information technology security checks, and many others.[146] These standards could help a company understand what reasonable industry practice is and provide the company with an argument for why their standards are reasonable in case of an FTC complaint. The ISO standards for information technology should be persuasive in adjudication with the FTC because the United States is both a participating country and the secretariat of the informational technology committee.[147]

Another independent source companies could use to establish reasonable data security practices through industry practice is the Institute of Electrical and Electronic Engineers (IEEE). The IEEE is the world's largest professional association dedicated to "advancing technological innovation and excellence for the benefit of humanity."[148] The IEEE consists of technical professionals such as engineers, scientists, software developers, information technology professionals, and many others.[149] The IEEE board creates standards for specific industries and technologies that are available for purchase online.[150] As with the ISO standards, companies could incorporate IEEE standards as the reasonable industry standards when FTC guidelines are not sufficient. The IEEE standards could also provide a persuasive argument in adjudication that a company was upholding reasonable data security practices based on industry standard.

B. In Case of an FTC Complaint: Comply and Consent

So what should businesses do if they find themselves on the receiving end of an FTC complaint due to a data security breach? Businesses and their legal counsel can either comply, settle and sign a consent order, or fight the FTC's authority through the judiciary. As evident through the lack of adjudicated cases, most businesses have chosen to settle and sign consent orders.[151] Most businesses choose to settle because the financial penalties paid in settlement cost much less than fighting the FTC because the business avoids lengthy

143. *About ISO*, ISO, http://www.iso.org/iso/home/about.htm (last visited Nov. 11, 2015).

144. *Technical Committees*, ISO, http://www.iso.org/iso/home/standards_development/list_of_iso_technical_committees.htm (last visited Nov. 11, 2015).

145. *Standards Catalogue*, ISO, http://www.iso.org/iso/home/store/catalogue_tc/catalogue_tc_browse.htm?commid=45306&published=on (last visited Nov. 11, 2015).

146. *Id.*

147. *ISO/IEC JTC 1–Information Technology*, ISO, http://www.iso.org/iso/home/standards_development/list_of_iso_technical_committees/iso_technical_committee_participation.htm?commid=45020 (last visited Nov. 11, 2015).

148. *About IEEE*, IEEE, https://www.ieee.org/about/index.html (last visited Nov. 11, 2015).

149. *See History of IEEE*, IEEE, https://www.ieee.org/about/ieee_history.html?WT.mc_id=lp_ab_hoi (last visited Nov. 11, 2015) (explaining "[i]t is designed to serve professionals involved in all aspects of the electrical, electronic, and computing fields, and related areas of science and technology that underlie modern civilization").

150. *IEEE Standards Association*, IEEE, standards.ieee.org/index.html (last visited Nov. 11, 2015).

151. *Supra* Section II.C; *see also* Solove & Hartzog, *supra* note 26, at 610–11 (stating out of the 170 FTC privacy-related complaints, only one resulted in a judicial opinion). Google, Facebook, Myspace, Sears, and Sony have all recently entered into consent orders with the FTC regarding data securities issues. *Id.* at 615–24.

litigation.[152] Businesses also settle to avoid reputational costs.[153] Settlements do not come without a cost. Typical consent orders last 20 years—meaning companies must file reports of compliance and are subjected to inspection for twenty years[154]—but there is potential for orders to be interpreted as perpetual if the order does not list a termination date.[155] If a company violates a consent order, each violation can cost up to $16,000.[156] The FTC assessed a $22.5 million fine against Google for multiple violations of a consent order—the largest fine ever assessed for such violations.[157]

Despite the plausible fair notice arguments, businesses should continue to settle FTC complaints, especially given the recent opinion in *Wyndham*, which indicates businesses will lose litigation battles.[158] Three main reasons support why the *Wyndham* court's decision is a good indicator of future court decisions. First, the court correctly relied on important precedent,[159] *FTC v. Sperry & Hutchinson Co.*, which held Congress intended to grant the FTC broad discretionary power.[160] Congress designed the Commission to serve as experts on issues of the market;[161] thus, courts have deferred to the FTC's discretion in determining what constitutes an unfair or deceptive business practice.[162]

Second, the *Wyndham* court correctly relied on precedent that defers to agency decisions to create standards either through formal rulemaking or adjudication.[163] The courts have upheld agency power to decide how to articulate standards of regulation to allow agencies to respond to unseen situations, develop expertise in an area before issuing a rule, and allow for agencies to maintain flexibility in regulations.[164] Congress purposefully granted the FTC fluid jurisdiction in order to regulate the "constant evolution of business practice and norms."[165]

Third, the lack of congressional action to stop the FTC from pursuing data security issues also presents another reason businesses would be fighting an uphill battle against the FTC. Agency power to regulate stems from Congress;[166] thus, unless Congress specifically indicates data security regulations do not fall under the FTC's broad powers,

---

152. Solove & Hartzog, *supra* note 26, at 611–13. The cost of a FTC fine usually ranges in the thousands of dollars. *Id.* at 612. Therefore, the cost of the fine would be less than a business paying a legal team to defend their company for years. For example, consider the legal bill of LabMD, who has two firms (Kilpatrick Townsend & Stockton, LLP and Dinsmore & Shohl, LLP) handling its ongoing two-year battle. LabMD, Inc. v. FTC, 776 F.3d 1275, 1275 (11th Cir. 2015).

153. Solove & Hartzog, *supra* note 26, at 613.

154. Stegmaier & Bartnick, *supra* note 106, at 22.

155. Solove & Hartzog, *supra* note 26, at 614.

156. Stegmaier & Bartnick, *supra* note 106, at 22.

157. *Id.*

158. FTC v. Wyndham Worldwide Corp., No 14-3514, 2015 WL 4998121, at *1 (3d Cir. Aug. 24, 2015).

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

160. Robert A. Skitol, *How BC and BCP Strengthen Their Respective Policy Missions Through New Uses of Each Other's Authority*, 72 ANTITRUST L.J. 1167, 1169 (2005); *see also* FTC v. Sperry & Hutchinson Co., 405 U.S. 233, 242 (1972) (stating the FTC has broad powers to decide what are unfair practices).

161. Christian Carlson, *Antitrusting the Federal Trade Commission: Why Courts Should Defer to the Federal Trade Commission in Antitrust Decision Making*, 12 DEPAUL BUS. & COM. L.J. 361, 367 (2014).

162. *See, e.g.*, *Sperry*, 405 U.S. at 245 (stating "legislative and judicial authorities alike convince us that the Federal Trade Commission does not arrogate excessive power to itself if, in measuring a practice against the elusive, but congressionally mandated standard of fairness").

163. *Wyndham*, 10 F. Supp. 3d at 617.

164. *Id.* (citing SEC v. Chenery Corp., 332 U.S. 194, 203 (1947)).

165. Frechette, *supra* note 10, at 1413.

166. *Wyndham*, 10 F. Supp. 3d at 615.

the deference given to the FTC assumes Congress intended the FTC to regulate data security. The FTC has been pursuing data security issues since 2005, yet no congressional action has indicated the area to be outside of the FTC's power.[167] Unless Congress passes legislation regarding the FTC's authority over data regulations, the FTC could expand and begin regulating more aggressively.[168]

Since the *Wyndham* court correctly analyzed the FTC's authority, fighting the FTC in court will only end up costing businesses litigation expenses without getting favorable judicial opinions. Businesses, however, should not give up and simply hope they guessed correctly in having reasonable data security practices. Businesses need to push Congress for legislation which either allows the FTC to make rules through regular APA processes (rather than Magnuson-Moss rulemaking) or creates a regulatory guide for businesses to follow. Large corporations should lobby for better legislation for data security regulations given their large amount of resources. Attorneys should advise small and medium businesses of the serious risks and consequences of having poor data security practices. Small and medium sized companies are at more of a risk than large corporations because they may not be able to pay either the fines to settle or the cost to litigate without going under. The law places businesses in an unpredictable and difficult position by holding them accountable to an unclear standard of reasonable data security practices. Businesses will likely not attain a change of law through litigation; so, for now, they must comply to the best of their ability and lobby Congress to clarify data security practice standards.

167. Bender, *supra* note 13, at 1674.
168. Solove & Hartzog, *supra* note 26, at 676.