William & Mary Law Review

Volume 58 | Issue 6 Article 7

A Case of Overcorrection: How the FTC's Regulation of "Unfair Acts And Practices" is Unfair to Small Businesses

Jennifer L. West

A CASE OF OVERCORRECTION: HOW THE FTC'S REGULATION OF "UNFAIR ACTS AND PRACTICES" IS UNFAIR TO SMALL BUSINESSES

TABLE OF CONTENTS

INTRODUCTION

The Federal Trade Commission (FTC) has used section 5 of the Federal Trade Commission Act of 1914 (FTC Act) to regulate companies' data security practices since 2002.[1] Section 5 of the FTC Act empowers the FTC to regulate "unfair or deceptive acts or practices."[2] When the FTC first began using this power in the realm of data security, it focused on its deceptiveness power rather than its unfairness power.[3] The deceptiveness power permits the FTC to investigate cases involving "a representation, omission or practice that is likely to mislead the consumer."[4] In the realm of data security, the FTC uses this power to file complaints against companies who have "deceived" consumers by violating their own privacy policies.[5] The problem is that when companies have exercised poor data security practices but have not violated their internal privacy policies—either because their policies are not comprehensive enough or because they do not have a privacy policy at all—those practices are not considered "deceptive" and thus are beyond the FTC's reach under its deceptiveness power.[6] As a result, the FTC has broadened

---

1. *See* 15 U.S.C. § 45(a)(1) (2012); FED. TRADE COMM'N, COMMISSION STATEMENT MARKING THE FTC'S 50TH DATA SECURITY SETTLEMENT 1 (2014), https://www.ftc.gov/system/files/documents/cases/140131gmrstatement.pdf [https://perma.cc/6HDW-EKD4]; Michael D. Scott, *The FTC, the Unfairness Doctrine, and Data Security Breach Litigation: Has the Commission Gone Too Far?*, 60 ADMIN. L. REV. 127, 129 (2008).

2. 15 U.S.C. § 45(a)(1).

3. *See* Letter from James C. Miller III, Chairman, Fed. Trade Comm'n, to the Honorable John D. Dingell, Chairman, Comm. on Energy & Commerce, U.S. House of Representatives (Oct. 14, 1983) [hereinafter FTC POLICY STATEMENT ON DECEPTION], *appended to* Clifford Assocs., Inc., 103 F.T.C. 110 app. at 174 (1984); *see also* Gerard M. Stegmaier & Wendell Bartnick, Essay, *Psychics, Russian Roulette, and Data Security: The FTC's Hidden Data-Security Requirements*, 20 GEO. MASON L. REV. 673, 674-75 (2013).

4. *See* FTC POLICY STATEMENT ON DECEPTION, *supra* note 3, at app. at 174-75.

5. *See* Scott, *supra* note 1, at 129; Stegmaier & Bartnick, *supra* note 3, at 674; *cf.* FTC POLICY STATEMENT ON DECEPTION, *supra* note 3, at app. at 175 ("Practices that have been found misleading or deceptive in specific cases include false oral or written representations, ... sales of hazardous or systematically defective products or services without adequate disclosures, ... failure to perform promised services, and failure to meet warranty obligations.").

6. *Cf.* J. Howard Beales III, *The Federal Trade Commission's Use of Unfairness Authority: Its Rise, Fall, and Resurrection*, 22 J. PUB. POL'Y & MARKETING 192, 192 (2003) ("Now, however, the FTC is using unfairness to attack practices that cause substantial injury but that could not be reached under deception theory, at least not without twisting the meaning of deception.").

its own reach by filing data security complaints under its unfairness power.[7]

The FTC uses a three-prong test, codified in 1994,[8] for finding unfair acts or practices in data security cases.[9] Under that test, the injury (1) "must be substantial"; (2) "must not be outweighed by any countervailing benefits to consumers or competition that the practice produces"; and (3) "must be an injury that consumers themselves could not reasonably have avoided."[10] Despite the FTC having initiated more than fifty data security proceedings since 2002,[11] this unfairness test remains vague and largely unsettled.[12]

The FTC's current application of the unfairness test is harmful to competition because it imposes a substantial burden on small businesses and hinders them from successfully competing in the market.[13] Due to the vague nature of the unfairness test, small businesses cannot anticipate what constitutes a breach and therefore cannot ensure that their practices pass FTC muster.[14] Consequently, small businesses either avoid taking risks and shy away from innovation, or they face the FTC's hefty settlement demands, which are not adequately tailored to the size and resources of each business.[15] Either way, the FTC's current practices harm competition by making small businesses unwilling or unable to compete in any meaningful way.[16]

Although the FTC claims it tailors its data security regulation to individual companies' particular circumstances,[17] in practice its

---

7. *See infra* Part II.C.

8. Federal Trade Commission Act Amendments of 1994, Pub. L. No. 103-312, § 9, 108 Stat. 1691, 1695 (codified as amended at 15 U.S.C. § 45(n)).

9. *See* Beales, *supra* note 6, at 195.

10. *Id.* at 194 (quoting FTC POLICY STATEMENT ON UNFAIRNESS, *infra* note 44, at app. at 1070, 1073).

11. *See* FED. TRADE COMM'N, *supra* note 1, at 2.

12. *See* Joshua D. Wright, Comm'r, Fed. Trade Comm'n, Section 5 Revisited: Time for the FTC to Define the Scope of Its Unfair Methods of Competition Authority, Remarks at the Symposium on Section 5 of the Federal Trade Commission Act 5-6 (Feb. 26, 2015), https://www.ftc.gov/system/files/documents/public_statements/626811/150226bh_section_5_symposium.pdf [https://perma.cc/29UD-NDWW].

13. *See infra* Part III.A.2.

14. *See infra* Part III.A.1.

15. *See infra* Part III.A.3.

16. *See infra* Part III.A.

17. *See* Stegmaier & Bartnick, *supra* note 3, at 693-94.

settlement agreements with various companies are all nearly identical.[18] Each settlement involves what is known as a "consent order" or "consent decree," in which a company agrees to implement typically twenty years of costly and time-consuming corrective data security measures.[19] These measures are problematic because they are far too costly for small businesses that do not have the manpower or money to implement them.[20]

Even though businesses technically "agree" to these consent decrees through settlement, the FTC essentially forces them into these agreements because these businesses have little ability or incentive to litigate.[21] This problem is especially true for small businesses for two principal reasons. First, litigation is too expensive and time-consuming.[22] For example, the cost of litigation in *FTC v. LabMD, Inc.*, effectively shut down a business.[23] LabMD, Inc., is an Atlanta-based cancer-detecting laboratory[24] that used to test specimen samples taken from patients by their health care providers.[25] The FTC filed a complaint against LabMD for a potential breach of patient information when a third party found the personal information of some of LabMD's patients on Limewire, a peer-to-peer (P2P) file-sharing network.[26] Instead of signing a consent decree like almost every other company, LabMD challenged the FTC through litigation.[27] Ultimately, the FTC won the battle.[28] LabMD no longer accepts new patients and merely exists to preserve test samples and to make available past test results.[29]

18. *See infra* Part II.A.
19. *See infra* Part II.A.
20. *See infra* Part III.A.1.
21. *See infra* Part II.A.
22. *See infra* Part II.B.
23. *See* Dan Epstein, Opinion, *Hounded Out of Business by Regulators*, WALL STREET J. (Nov. 19, 2015, 7:11 PM), http://www.wsj.com/articles/hounded-out-of-business-by-regulators-1447978301 [https://perma.cc/L4KF-PXKY].
24. *Id.*
25. *See* Complaint [Provisionally Redacted Public Version], LabMD, Inc., F.T.C. Docket No. 9357, at 1 (Aug. 29, 2013), https://www.ftc.gov/sites/default/files/documents/cases/2013/08/130829labmdpart3.pdf [https://perma.cc/BF8Z-2G68].
26. *See id.* at 4.
27. *See infra* Part II.B.
28. *See* Epstein, *supra* note 23.
29. *See* Opinion of the Commission, LabMD, Inc., F.T.C. Docket No. 9357, at 4 (July 28, 2016), https://www.ftc.gov/system/files/documents/cases/160729labmd-opinion.pdf [https://perma.cc/X8HS-CG5V] (discussing the current business state of LabMD).

Additionally, LabMD must now adhere to one of the FTC's twenty-year data security plans that is included in every consent decree.[30]

The second reason small businesses have little ability or incentive to litigate is that the FTC benefits from tremendous institutional bias.[31] Even though the administrative law judges (ALJs) are separate from the investigative arm of the FTC, that bias still apparently exists because the FTC has affirmed judgment in every case in which the ALJ found in favor of the FTC staff, but has reversed judgement in every case in which the ALJ found against the FTC staff.[32]

If the FTC continues to use its unfairness power in this way, then it will harm competition by running smaller businesses out of the market, leaving the big businesses that can afford to settle with the FTC as market monopolies.[33] Ultimately, consumers will be left without adequate, affordable choices for all types of products and services.[34]

To remedy this problem, the FTC should apply a framework similar to the antitrust rule of reason to the balancing prong of its unfairness test—that is, the harm to consumers must not be "outweighed by countervailing benefits to consumers or to competition."[35] The antitrust rule of reason consists of a burden-shifting analysis focused on competitive effects of particular acts or practices.[36] For purposes of the unfairness test, the FTC should focus on whether its own methods of regulating data security acts or practices are actually anticompetitive by forcing companies out of the market.[37] By considering these effects, the FTC will be forced to more adequately tailor its regulation of data security to the size and

30. Final Order, LabMD, Inc., F.T.C. Docket No. 9357 (July 28, 2016), https://www.ftc.gov/system/files/documents/cases/160729labmdorder.pdf [https://perma.cc/ERA3-5TXT]; *see also infra* Part II.A (discussing the identical nature of the FTC's consent decrees).

31. *See* Wright, *supra* note 12, at 6-7 (discussing and presenting evidence of the institutional bias).

32. *See id.* at 6 n.2 (data reported from Aug. 2013); *see also* Final Order, LabMD, Inc., *supra* note 30, at 1 (reversing Chief A.L.J. D. Michael Chappell's Initial Order that held there was no violation on the part of LabMD).

33. *See infra* Part III.A.

34. *See infra* Part III.A.

35. 15 U.S.C. § 45(n) (2012).

36. *See infra* Part III.B.

37. *See infra* Part III.B.

resources of each business. This modification will give the FTC's largely ad hoc approach a great deal more consistency and will benefit competition—and therefore consumers—in the long term.

Part I of this Note discusses the FTC's power to regulate data security. It surveys the history of the FTC's section 5 authority generally and how the FTC began to use this authority in data security cases. Part II details the data security cases the FTC has pursued under section 5. It discusses the settlements, or "consent decrees," the FTC has entered into with various companies, the two major cases that challenged the FTC's data security complaints and underwent extensive litigation, and the unfairness test as it stands today. Part III explores the problems with the current analysis under the unfairness test and the corresponding potential harms to smaller businesses. Part III then proposes a new framework by discussing the antitrust rule of reason and follows with an explanation as to why this framework is better suited to deal with data security issues than the current framework.

I. HISTORY OF THE FTC'S UNFAIRNESS AUTHORITY IN DATA SECURITY CASES

A. Pre-1980

In the FTC Act, Congress established the FTC and charged it with preventing anticompetitive practices.[38] Congress later gave the FTC its broad unfairness authority when it amended section 5 of the FTC Act in 1938.[39] Also known as the Wheeler-Lea Act, this amendment made "[u]nfair methods of competition in commerce, and unfair or deceptive acts or practices in commerce" unlawful.[40] Under these provisions, the FTC held the authority to protect consumers directly by enforcing these provisions against businesses.[41]

38. *See* 15 U.S.C. § 45(a)(1); *see also About the FTC*, FED. TRADE COMMISSION, https://www.ftc.gov/about-ftc [https://perma.cc/YSH5-G2T9].

39. *See* Wheeler-Lea Act, ch. 49, sec. 3, § 5(a), 52 Stat. 111, 111 (1938) (codified as amended at 15 U.S.C. § 45(a) (2012)).

40. *Id.* ("Unfair methods of competition in or affecting commerce, and unfair or deceptive acts or practices in or affecting commerce, are hereby declared unlawful.").

41. Beales, *supra* note 6, at 192.

The FTC initially failed to distinguish between *unfair* acts or practices and *deceptive* acts or practices, and treated section 5 of the FTC Act as if the provision said "and," instead of "or."[42] In 1964 the FTC then distinguished between the two when it released the Cigarette Rule Statement of Basis and Purpose.[43] In that statement, the FTC summed up the unfairness test in three prongs: in cases involving unfair acts or practices, the FTC would consider "(1) whether the practice ... offends public policy as it has been established by statutes, the common law, or otherwise ... ; (2) whether it is immoral, unethical, oppressive, or unscrupulous; [and] (3) whether it causes substantial injury to consumers (or competitors or other businessmen)."[44]

In 1972 the Supreme Court in *FTC v. Sperry & Hutchinson Co.* took the position that section 5 "empower[s] the Commission to define and proscribe an unfair competitive practice, even though the practice does not infringe either the letter or the spirit of the antitrust laws."[45] Section 5 also "empower[s] the Commission to proscribe practices as unfair or deceptive in their effect upon consumers regardless of their nature or quality as competitive practices or their effect on competition."[46]

Although the Supreme Court approved of the FTC's broad power, it still failed to provide the FTC with any guidance for applying

---

42. *See id.*

43. Unfair or Deceptive Advertising and Labeling of Cigarettes in Relation to the Health Hazards of Smoking, 29 Fed. Reg. 8324, 8354 (July 2, 1964) ("[T]he prohibitions of section 5 of the Trade Commission Act embrace acts, practices, or methods of competition that are neither deceptive or misleading, on the one hand, nor monopolistic or anticompetitive, on the other."); *see also* Beales, *supra* note 6, at 192-93 ("[I]n the Cigarette Rule SBP, the commission set forth a test for determining whether an act or practice is 'unfair.'").

44. Letter from Michael Pertschuk, Chairman, Fed. Trade Comm'n et al., to the Honorable Wendell H. Ford & the Honorable John C. Danforth, Consumer Subcomm., Comm. on Commerce, Sci. & Transp., U.S. Senate, Commission Statement of Policy on the Scope of the Consumer Unfairness Jurisdiction (Dec. 17, 1980) [hereinafter FTC POLICY STATEMENT ON UNFAIRNESS] (quoting Unfair or Deceptive Advertising and Labeling of Cigarettes in Relation to the Health Hazards of Smoking, 29 Fed. Reg. at 8355), *appended to* Int'l Harvester Co., 104 F.T.C. 949 app. at 1070, 1072 n.8 (1984).

45. 405 U.S. 233, 239 (1972).

46. *Id.* This was despite the Supreme Court's reversal of the FTC's prior ruling. *See* Beales, *supra* note 6, at 193 & n.5 ("Proceedings before the FTC were based on the theory that Sperry & Hutchinson was engaged in an unfair *method of competition*. On appeal, the Commission argued that Sperry & Hutchinson was engaged in unfair *practices*. The Court reversed and remanded because the case was not tried under an unfair practices theory.").

these three prongs.[47] For the next eight years, the FTC inconsistently applied its unfairness power in a variety of cases.[48] To solve this problem and to answer questions from Congress and many others, the FTC passed the FTC Policy Statement on Unfairness in 1980.[49] In this statement, the FTC declared that "[u]njustified consumer injury is the primary focus of the FTC Act, and the most important of the three [*Sperry & Hutchinson*] criteria."[50] In fact, the FTC stated that it could find that an act or practice was unfair based on unjustified consumer injury alone.[51] Yet that "[did] not mean that every consumer injury [was] legally 'unfair.'"[52] Consequently, the FTC set forth a different unfairness test than the one it articulated in 1964: the injury (1) "must be substantial"; (2) "must not be outweighed by any countervailing benefits to consumers or competition that the practice produces"; and (3) "must be an injury that consumers themselves could not reasonably have avoided."[53]

The FTC codified this approach in 1994, "reestablish[ing] a cost-benefit analysis (injury to consumers not outweighed by countervailing benefits) as the test for unfairness," rather than the public-policy focus of the 1964 Cigarette Rule.[54] The codification is now section 5(n) of the FTC Act, which reads as follows:

> 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

47. *See* Beales, *supra* note 6, at 193.

48. *See id.*

49. *See id.* at 193-94.

50. FTC POLICY STATEMENT ON UNFAIRNESS, *supra* note 44, at app. at 1073.

51. *Id.* (enabling the FTC to rely on consumer injury as an "independent criterion"). The FTC justified this position on the intent of the statute: to make "the consumer who may be injured by an unfair trade practice of equal concern before the law with the merchant injured by the unfair methods of a dishonest competitor." *Id.* (quoting 83 CONG. REC. 3255 (1938) (remarks of Sen. Wheeler)).

52. *Id.*

53. *Id.*

54. Beales, *supra* note 6, at 192-94.

> evidence to be considered with all other evidence. Such public policy considerations may not serve as a primary basis for such determination.[55]

After codification of the unfairness test, the FTC largely avoided using it for the remainder of the 1990s and began using it again only to reach cases of "substantial injury ... that could not be reached under deception theory."[56] One example of this is in the realm of data security cases.

B. Post-1980

Internet commerce grew rapidly in the mid-1990s, and "the Commission has been at the forefront of the public debate on online privacy" since 1995.[57] Initially, the FTC argued against Congress passing legislation to regulate online privacy.[58] Instead, the FTC pushed for industry self-regulation as the way to control online privacy issues.[59]

The FTC's idea of self-regulation involved companies voluntarily providing the FTC with copies of their "online information practice guidelines and principles."[60] Although some companies stepped up and began utilizing the online privacy practices the FTC had been hoping for, this approach ultimately proved ineffective.[61] Self-regu-

---

55. Federal Trade Commission Act Amendments of 1994, Pub. L. No. 103-312, § 9, 108 Stat. 1691, 1695 (codified as amended at 15 U.S.C. § 45(n) (2012)).

56. Beales, *supra* note 6, at 192.

57. *See* DIV. OF FIN. PRACTICES, FED. TRADE COMM'N, PRIVACY ONLINE: FAIR INFORMATION PRACTICES IN THE ELECTRONIC MARKETPLACE, A REPORT TO CONGRESS 1-3 (2000) [hereinafter FTC 2000 REPORT TO CONGRESS], https://www.ftc.gov/sites/default/files/documents/reports/privacy-online-fair-information-practices-electronic-marketplace-federal-trade-commission-report/privacy2000.pdf [https://perma.cc/89P4-29XU].

58. *See id.* at 34-35.

59. *See* BUREAU OF CONSUMER PROT., FED. TRADE COMM'N, PRIVACY ONLINE: A REPORT TO CONGRESS 41 (1998) [hereinafter FTC 1998 REPORT TO CONGRESS], https://www.ftc.gov/sites/default/files/documents/reports/privacy-online-report-congress/priv-23a.pdf [https://perma.cc/3K7Q-2WPU]; *see also* FTC 2000 REPORT TO CONGRESS, *supra* note 57, at 34-35 ("In its 1999 Report, a majority of the Commission again determined that legislation was not then appropriate, but noted the 'substantial challenges' that industry continued to face in implementing widespread self-regulation.").

60. FTC 1998 REPORT TO CONGRESS, *supra* note 59, at 15.

61. *See* FTC 2000 REPORT TO CONGRESS, *supra* note 57, at 35 ("Notwithstanding several years of industry and governmental effort, only 8% of heavily-trafficked Web sites display a seal from one of the self-regulatory seal programs.").

lation was unsuccessful because the FTC could not force companies to comply with its online privacy recommendations, including the recommendation that they should even have a policy in the first place.[62] As a result, after two years of trying to make self-regulation take hold in the business community, the FTC eventually pushed for Congress to pass legislation as a means of regulation.[63]

Shortly thereafter, the FTC reverted back to its old stance in support of a more aggressive approach on legislative regulation.[64] In a 2001 speech, FTC Chairman Timothy Muris announced the FTC's position on online privacy to protect consumers through "aggressive enforcement of the basic laws of consumer protection."[65]

One of the enforcement mechanisms Muris was talking about is the FTC's use of its deceptiveness power.[66] According to the FTC, a practice is deceptive when it involves "a representation, omission or practice that is likely to mislead the consumer."[67] The FTC uses its deceptiveness power under section 5 to investigate companies that have published their own privacy policies but have failed to follow them.[68] For example, in the FTC's case against Snapchat, Inc., a company known for its video and picture messaging application,[69] the FTC argued that Snapchat misrepresented how much data was collected from consumers and how it protected that data.[70] But this approach did not apply to all cases. If a corporation had not contra-

62. *See id.* at 34 ("As a general matter, however, 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.").

63. *See id.* at 36.

64. *See* Scott, *supra* note 1, at 131; *cf.* FTC 2000 REPORT TO CONGRESS, *supra* note 57, at 36-37 ("[T]he Commission recommends that any legislation be phrased in general terms and be technologically neutral. Thus, the definitions of fair information practices set forth in the statute should be broad enough to provide flexibility to the implementing agency in promulgating its rules or regulations.").

65. Scott, *supra* note 1, at 131 (quoting *Challenges Facing the Federal Trade Commission: Hearing on H.R. 68 Before the Subcomm. on Commerce, Trade, and Consumer Protection of the H. Comm. on Energy and Commerce*, 107th Cong. 12 (2001) (statement of Timothy J. Muris, FTC Chairman)).

66. *See id.*

67. FTC POLICY STATEMENT ON DECEPTION, *supra* note 3, at app. at 175.

68. *See* Peter S. Frechette, Note, FTC v. LabMD*: FTC Jurisdiction over Information Privacy Is "Plausible," but How Far Can It Go?*, 62 AM. U. L. REV. 1401, 1403-04 (2013).

69. *See Snap Inc.*, SNAP INC., https://www.snap.com/en-US/ [https://perma.cc/JA38-XGP2].

70. *See* Press Release, Fed. Trade Comm'n, FTC Approves Final Order Settling Charges Against Snapchat (Dec. 31, 2014), https://www.ftc.gov/news-events/press-releases/2014/12/ftc-approves-final-order-settling-charges-against-snapchat [https://perma.cc/UQN9-XU75].

dicted its data security policies, or if it had not enacted any such policies, then the FTC could not file a complaint under its deceptiveness power against that corporation.[71] As a result, the FTC attempted to expand its reach in data security cases by using its unfairness power to reach companies that maintained poor data security practices without having breached any data security policies.[72] This overreach resulted in numerous settlements with companies under investigation, including two major cases that apparently challenged the FTC's authority in vain.[73]

II. THE FTC'S DATA SECURITY CASES

A. Settlements and Consent Decrees

The FTC has settled more than fifty data security cases against private companies since 2002, and it has used either its deceptiveness power or its unfairness power in each case.[74] Some well-known examples include those against Snapchat, Inc.,[75] Twitter, Inc.,[76] CVS Pharmacy, Inc.,[77] DSW, Inc.,[78] and a number of other large corporations that have undergone major data breaches.[79] Almost every data

71. *Cf.* Beales, *supra* note 6, at 192 ("Now, however, the FTC is using unfairness to attack practices that cause substantial injury but that could not be reached under deception theory, at least not without twisting the meaning of deception.").

72. *See id.* at 195 ("The commission under Chairman Muris is now giving unfairness a more prominent role as a powerful tool for the commission to analyze and attack a wider range of practices that may not involve deception but nonetheless cause widespread and significant consumer harm.").

73. *See infra* Part II.B.

74. *See* FED. TRADE COMM'N, *supra* note 1; Alden F. Abbott, *The Federal Trade Commission's Role in Online Security: Data Protector or Dictator?*, HERITAGE FOUND. LEGAL MEMORANDUM, No. 137, Sept. 10, 2014, at 3, http://thf_media.s3.amazonaws.com/2014/pdf/LM137.pdf [https://perma.cc/R7RY-E8GQ].

75. *See* Decision & Order, Snapchat, Inc., F.T.C. Docket No. C-4501, at 1 (Dec. 23, 2014), https://www.ftc.gov/system/files/documents/cases/141231snapchatdo.pdf [https://perma.cc/YR3B-DUH4].

76. *See* Twitter, Inc., 151 F.T.C. 162, 170 (2011) (Decision & Order).

77. *See* Decision & Order, CVS Caremark Corp., F.T.C. Docket No. C-4259, at 1 (June 18, 2009), https://www.ftc.gov/sites/default/files/documents/cases/2009/06/090623cvsdo.pdf [https://perma.cc/4H2L-WLDL].

78. *See* DSW, Inc., 141 F.T.C. 117, 121 (2006) (Decision & Order).

79. For more FTC settlements, search under the topic "data security cases" on *Legal Resources*, FED. TRADE COMMISSION, https://www.ftc.gov/tips-advice/business-center/legal-resources?type=case&field_consumer_protection_topics_tid=249 [https://perma.cc/3QBV-SLYJ].

security case pursued by the FTC has ended in settlement.[80] These settlements involve what are known as "consent orders,"[81] or "consent decrees."[82] In a consent decree, "a company agrees to cease practices the FTC deems unlawful and to take various 'corrective measures' to prevent future harm."[83] Corrective measures may include "implementation of comprehensive privacy and security programs, biennial assessments by independent experts, monetary redress to consumers, disgorgement of ill-gotten gains, deletion of illegally obtained consumer information, and provision of robust notice and choice mechanisms to consumers."[84]

One example of a consent order can be found in the FTC's settlement with BJ's Wholesale Club, Inc.[85] BJ's Wholesale Club agreed to, among other actions, "establish and implement, and thereafter maintain, a comprehensive information security program that is reasonably designed to protect" consumer data and fully document virtually every detail of the program; "obtain an assessment and report ... from a qualified, objective, independent third-party professional" biennially for twenty years following the consent order; and to maintain any documents relating to compliance for a certain period of time depending on the document, as well as make those documents available to the FTC upon request.[86] This consent order is effective for twenty years "from the most recent date that the United States or the Federal Trade Commission files a complaint ... in federal court alleging any violation of the order, whichever comes later."[87]

---

80. *See* Jennifer Woods, *Federal Trade Commission's Privacy and Data Security Enforcement Under Section 5*, A.B.A. YOUNG LAW. DIV., http://www.americanbar.org/groups/young_lawyers/publications/the_101_201_practice_series/federal_trade_commissions_privacy.html [https://perma.cc/UQ4R-VS9R].

81. *See* Scott, *supra* note 1, at 133.

82. Abbott, *supra* note 74.

83. *Id.*

84. FED. TRADE COMM'N, 2014 PRIVACY AND DATA SECURITY UPDATE (2015) [hereinafter 2014 PRIVACY AND DATA SECURITY UPDATE], https://www.ftc.gov/system/files/documents/reports/privacy-data-security-update-2014/privacydatasecurityupdate_2014.pdf [https://perma.cc/3MCU-EQH6].

85. BJ's Wholesale Club, Inc., 140 F.T.C. 465, 469 (2005) (Decision & Order).

86. *Id.* at 471-73.

87. *Id.* at 475.

Another example of a consent order is the FTC's settlement with DSW, Inc.[88] DSW underwent a breach several months before the settlement that compromised the information of approximately 1,438,281 credit and debit card holders.[89] On December 1, 2005, the FTC filed a complaint against DSW alleging that this breach was a result of the company's inadequate business practices, namely its failure to better secure credit card information by deleting information that was no longer in use and by securing its computer network.[90] As a result, DSW entered into a settlement with the FTC whereby DSW agreed to implement and maintain a comprehensive security program "reasonably designed to protect the security, confidentiality, and integrity of personal information collected from or about consumers."[91] DSW also agreed to obtain biennial assessments from a qualified third party for twenty years after the consent order was implemented, to maintain each document related to compliance and make those documents available to the FTC upon request, to provide the consent order to any current and future employee of the company whose position is in any way related to the data security program, to file reports with the FTC at specified times, and to notify the FTC of any changes to the corporation that affect the data security program.[92]

What is striking about the FTC's consent decrees is that they are all nearly identical. For example, in the BJ's Wholesale Club and DSW cases, the consent decrees contained agreements to implement comprehensive security programs, biennially obtain assessments from third-party professionals, and make documents available to the FTC upon request.[93] Both consent decrees were also set to last for twenty years.[94] Not only are these provisions' mandates the same, but the language for each provision is very similar as well, indicating that the FTC applies the same, or at least nearly identical, provisions to each data security case.[95]

88. *See generally* DSW, Inc., 141 F.T.C. 117, 117-20 (2006) (Complaint).
89. *Id.* at 120.
90. *Id.* at 119.
91. *Id.* at 123 (Decision & Order).
92. *Id.* at 124-27.
93. *Id.* at 123-26; BJ's Wholesale Club, Inc., 140 F.T.C. 465, 471-73 (2005).
94. *DSW, Inc.*, 141 F.T.C. at 127; *BJ's Wholesale Club, Inc.*, 140 F.T.C. at 475.
95. *Compare DSW, Inc.*, 141 F.T.C. at 123-27, *with BJ's Wholesale Club, Inc.*, 140 F.T.C. at 470-75. *See also* Twitter, Inc., 151 F.T.C. 162, 172-77 (2011) (Decision & Order); Decision

Although companies "agree" to these corrective measures, they do not have much bargaining power. The final consent decrees are nearly identical to the orders the FTC provides companies when it first files a complaint.[96] This is a further indication of the fact that the FTC has institutional advantages over companies, and it shows that consent decrees are boilerplate settlements that leave companies little room for negotiation.[97] Despite this, only a few companies refused to sign a consent order and, instead, took their cases all the way to trial.[98]

B. Litigation: FTC v. Wyndham Worldwide Corp. *and* FTC v. LabMD, Inc.

FTC v. Wyndham Worldwide Corp. and *FTC v. LabMD, Inc.*, are two examples of cases in which the companies under investigation did not settle with the FTC.[99] Rather than agreeing to sign consent orders, Wyndham and LabMD challenged the FTC's complaints against them, as well as the FTC's general authority to regulate data security under its section 5 unfairness power.[100]

In *Wyndham*, hackers gained access to Wyndham's computer systems on three occasions between 2008 and 2009.[101] The FTC alleged that the breaches were a result of Wyndham's unfair and deceptive security practices,[102] which "taken together, unreasonably

---

& Order, CVS Caremark Corp., *supra* note 77, at 3-6. For more examples of these consent decrees, search under the topic "data security cases" at *Legal Resources*, FED. TRADE COMMISSION, https://www.ftc.gov/tips-advice/business-center/legal-resources?type=case&field_consumer_protection_topics_tid=249 [https://perma.cc/3QBV-SLYJ].

96. *Compare* Complaint, *supra* note 25, at 7-12, *and* Agreement Containing Consent Order, BJ's Wholesale Club, Inc., F.T.C. Matter No. 0423160, at 2-6 (May 17, 2005), https://www.ftc.gov/sites/default/files/documents/cases/2005/06/050616agree0423160.pdf [https://perma.cc/VDZ6-9ES9], *with* Final Order, LabMD, Inc., *supra* note 30, *and BJ's Wholesale Club, Inc.*, 140 F.T.C. at 470-75.

97. *See* Wright, *supra* note 12, at 7 (asserting that the FTC has an institutional advantage over companies).

98. *See infra* Part II.B.

99. *See generally* FTC v. Wyndham Worldwide Corp., 799 F.3d 236 (3d Cir. 2015); Opinion of the Commission, LabMD, Inc., *supra* note 29.

100. *See Wyndham*, 799 F.3d at 243-48; Initial Decision, LabMD, Inc., F.T.C. Docket No. 9357, at 3 (Nov. 13, 2015), https://www.ftc.gov/system/files/documents/cases/151113labmd_decision.pdf [https://perma.cc/A62V-W7CL].

101. *Wyndham*, 799 F.3d at 240-42.

102. *Id.* at 240.

and unnecessarily exposed consumers' personal data to unauthorized access and theft."[103] Wyndham filed a motion to dismiss the section 5 claims, but the district court denied the motion and the Third Circuit granted Wyndham's application for appeal.[104] In its August 24, 2015, decision, the Third Circuit denied Wyndham's motion to dismiss.[105]

Wyndham made three major arguments: (1) the FTC had no congressional authority to regulate cybersecurity; (2) the complaint was a violation of the Due Process Clause of the Fourteenth Amendment because the FTC failed to give companies fair notice of what would constitute a breach; and (3) the three unfairness prongs were necessary but not sufficient factors to consider in unfairness cases.[106] In response, the Third Circuit noted that Congress gave the FTC its authority to regulate cybersecurity when it enacted the FTC Act, and that subsequent congressional action had not taken away that authority.[107] Additionally, the Third Circuit held that the FTC gave fair notice that Wyndham's practices might be in violation of section 45(a) simply by virtue of its language.[108] It noted that statutory ambiguity does not necessitate a lack of fair notice.[109]

Yet, the Third Circuit did not fully discount all of Wyndham's arguments. The court concluded by saying the three unfairness prongs may, in fact, "be necessary rather than sufficient conditions" for proving unfair acts or practices.[110] Although the Third Circuit still affirmed the district court's holding,[111] this opinion leaves the extent of the FTC's section 5 power open to more challenges. The Third Circuit indicated that *Wyndham* was an easy case in which to find unfair security practices.[112] The court emphasized that "Wyndham's as-applied challenge [fell] well short given the allegations in

103. *Id.* (quoting Complaint for Injunctive and Other Equitable Relief ¶ 24, *Wyndham*, 799 F.3d 236 (No.14-3514), https://www.ftc.gov/sites/default/files/documents/cases/2012/06/120626wyndamhotelscmpt.pdf [https://perma.cc/E96C-PQK5]).

104. *See id.* at 242 (removing the case from the U.S. District Court for the District of Arizona to the U.S. District Court for the District of New Jersey).

105. *Id.* at 259.

106. *See id.* at 244-49.

107. *Id.* at 243-44, 247-49.

108. *Id.* at 255-56, 259.

109. *Id.* at 252.

110. *Id.* at 259.

111. *See id.*

112. *Id.* at 256.

the FTC's complaint" because, rather than arguing that Wyndham had weak data security measures, the FTC argued that Wyndham failed to use firewalls, encryption software, IP address restrictions, or other security measures at all.[113] The court also emphasized that Wyndham's system was hacked "not one or two, but three, times."[114] *Wyndham* does not give sufficient guidance for cases involving less obvious breaches or data security issues because this case included such strong evidence of a major breach in data security.

Moreover, Wyndham settled after the Third Circuit denied its motion to dismiss, leaving the issues ultimately undecided.[115] Thus, *Wyndham* is not the be-all, end-all of the FTC's power to regulate data security under section 5. Alden Abbott, a former director of antitrust for the FTC,[116] argued that the *Wyndham* decision

> in no way alters the fact that the FTC's existing cybersecurity enforcement program is inadequate and unsound. Whether through guidelines or formal FTC rules ... the FTC should provide additional guidance to the private sector, *rooted in sound cost-benefit analysis*. The FTC should also be ever mindful of the costs it imposes on the economy (including potential burdens on business innovation) whenever it considers bringing enforcement actions in this area.[117]

Another company that challenged the FTC's authority is LabMD, Inc.[118] LabMD is a small cancer detection lab in Atlanta, Georgia,

---

113. *Id.*

114. *Id.*

115. *See Wyndham Settles FTC Charges It Unfairly Placed Consumers' Payment Card Information at Risk*, FED. TRADE COMMISSION (Dec. 9, 2015, 12:00 PM), https://www.ftc.gov/news-events/press-releases/2015/12/wyndham-settles-ftc-charges-it-unfairly-placed-consumers-payment [https://perma.cc/H63P-CLP6].

116. Alden Abbott is the Deputy Director of the Edwin Meese III Center for Legal and Judicial Studies and the John, Barbara, and Victoria Rumpel Senior Legal Fellow at the Heritage Foundation. *Alden Abbott*, HERITAGE FOUND., http://www.heritage.org/about/staff/a/alden-abbott [https://perma.cc/AM7D-G8FT].

117. Alden Abbott, *Wyndham Decision Highlights FTC Role in Cybersecurity: Legal and Policy Considerations*, TRUTH ON MKT. (Sept. 1, 2015) (emphasis added), http://truthonthemarket.com/2015/09/01/wyndham-decision-highlights-ftc-role-in-cybersecurity-legal-and-policy-considerations/ [https://perma.cc/893M-T7FQ].

118. *See* Respondent LabMD, Inc.'s Answer and Defenses to Administrative Complaint, LabMD, Inc., F.T.C. Docket No. 9357, at 1 (Sept. 17, 2013), https://www.ftc.gov/system/files/documents/cases/578519.pdf [https://perma.cc/U47K-32ZL].

that used to test specimen samples sent by health care providers.[119] LabMD opened in 1966 and had a mere twenty employees.[120] In May 2008, a third party informed LabMD that the personal information of about 9300 patients was available on a P2P network, Limewire, an application commonly used to share music, videos, and pictures.[121] The billing department manager had downloaded Limewire to the company's billing computer no later than 2006, and upon learning of the wide availability of its information on the network in May 2008, LabMD immediately removed the application from the computer.[122] Four years later, in October 2012, California convicted several individuals on charges of identity theft after the Sacramento Police Department found certain LabMD day sheets and a few copied checks, payable to LabMD, in their possession.[123]

The FTC filed a complaint against LabMD in August 2013, alleging that LabMD violated the unfairness provision of section 5 by failing to put in place reasonable and appropriate data security measures.[124] Like Wyndham, LabMD attempted to have the complaint dismissed, arguing that LabMD did not engage in unfair practices and that the FTC did not have the power to regulate data security under section 5 of the FTC Act.[125] Chief ALJ D. Michael Chappell found that the FTC has congressional authority to regulate data security, that it has repeatedly affirmed its authority by filing actions in data security cases, and that no other legislation has precluded the FTC from bringing such actions.[126] Further, Chappell held that the FTC had the discretion to apply the unfairness doctrine on a case-by-case basis, and that this case did not

119. *See* Complaint, *supra* note 25, at 1; Abbott, *supra* note 74, at 5.

120. Cheryl Conner, *When the Government Closes Your Business*, FORBES (Feb. 1, 2014, 5:55 PM), http://www.forbes.com/sites/cherylsnappconner/2014/02/01/when-the-government-closes-your-business/ [https://perma.cc/M3ZE-YFQ4].

121. Complaint, *supra* note 25, at 4.

122. *Id.* at 4-5.

123. *Id.* at 5.

124. *Id.*

125. Respondent LabMD, Inc.'s Answer and Defenses to Administrative Complaint, *supra* note 118, at 1, 6.

126. Order Denying Respondent LabMD's Motion to Dismiss, LabMD, Inc., F.T.C. Docket No. 9357, at 3, 6, 10 (Jan. 16, 2014), https://www.ftc.gov/sites/default/files/documents/cases/140117labmdorder.pdf [https://perma.cc/EVF8-ESNZ].

violate LabMD's due process right under the Fourteenth Amendment.[127]

As for whether LabMD engaged in unfair practices, Chappell initially held that it did not.[128] He noted that even if harm was "possible," the FTC did not establish that substantial harm was "likely" to occur, which is the first requirement under the unfairness test.[129] He reasoned that the patient information was only available for a short time, and that any harm that could have occurred was subjective and speculative.[130] Chappell also found that the FTC did not provide sufficient evidence to find that the theft of the day sheets and checks from the California incident were in any way connected to the P2P file-sharing network or a lack of data security measures.[131] Much of the stolen information was not in the P2P file, and some of the information was actually stolen before LabMD started inputting the data in question.[132]

The FTC appealed, and a majority of the commission members—including Chairwoman Edith Ramirez, Maureen K. Ohlhausen, and Terrell McSweeny—reversed the initial decision and released a final order and a corresponding opinion statement on July 28, 2016.[133] The Commission first held that actual harm resulted from the unauthorized disclosure of sensitive health or medical information.[134] It then considered, notwithstanding its holding, that substantial harm to consumers was likely, and that Chappell followed the wrong standard in determining this prong of the unfairness test.[135] The Commission ultimately found that LabMD engaged in unfair data security practices because it did not train its IT personnel or its other employees on proper data security practices, and that it did not maintain adequate monitoring practices, such as installing software that could detect vulnerabilities in the system.[136]

---

127. *Id.* at 15.
128. Initial Decision, LabMD, Inc., *supra* note 100, at 88.
129. *Id.* at 54-55.
130. *Id.* at 85.
131. *Id.* at 13.
132. *See id.* at 72-73.
133. Final Order, LabMD, Inc., *supra* note 30, at 1; Opinion of the Commission, LabMD, Inc., *supra* note 29, at 1.
134. Opinion of the Commission, LabMD, Inc., *supra* note 29, at 19.
135. *Id.* at 20-21, 25.
136. *Id.* at 11-15.

The only matter on which the Commission agreed with Chappell was that there was not enough information to determine that the California incident was LabMD's fault.[137]

LabMD spent so much money on litigation that it had no choice but to stop accepting new patients and to begin winding down operations in January 2014.[138] It now exists merely to store test results from previous patients and provide those results upon request.[139] What is striking about the final order, and what makes it so surprising when compared to *Wyndham*, is that LabMD was not a large company conducting business in a large geographic area; rather, LabMD was a small business with only twenty employees.[140] Furthermore, the 9300 patient files on the P2P network constituted only 1 percent of its patient information,[141] the file was available only for a short time, and LabMD removed the software as soon as it learned that an employee had downloaded it onto one of LabMD's computers.[142] In contrast, Wyndham is a large, international company that accumulates more and more credit card information every day.[143] The potential for harm was enormous, and Wyndham underwent three major data security breaches.[144] Despite these differences, LabMD never stood a chance against the FTC.

LabMD underscores the FTC's tremendous institutional bias.[145] Former Commissioner Joshua D. Wright noted in February 2015 that "in 100 percent of cases where the administrative law judge ruled in favor of the FTC staff, the Commission affirmed liability; and in 100 percent of the cases in which the administrative law judge ... found no liability, the Commission reversed."[146] This institutional bias could serve as grounds for other companies to challenge the FTC's section 5 unfairness power in future data security cases.

---

137. *See id.* at 25.

138. *See id.* at 4.

139. *See id.*

140. Conner, *supra* note 120.

141. Initial Decision, LabMD Inc., *supra* note 100, at 20 (noting that LabMD stored the personal information of a total of 750 thousand patients).

142. *Id.* at 65.

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

144. *Id.* at 241-42.

145. *See* Wright, *supra* note 12, at 6-7 (discussing the FTC's institutional bias).

146. *Id.* at 6. This statistic held true for LabMD, as well. *See* Final Order, LabMD, Inc., *supra* note 30, at 1 (reversing the ALJ's dismissal of the FTC's complaint against LabMd).

C. The Unfairness Test Today

In data security cases, the FTC applies the same unfairness test it codified in 1994:

> The Commission shall have no authority under this section or section 57a of this title 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.[147]

The FTC has had little opportunity to reveal how it applies the unfairness test because almost every one of its data security cases has ended in a settlement.[148] Businesses have only two sources from which to draw information when attempting to discern how the FTC will apply this test: the few data security cases that have challenged the FTC and the few pieces of literature the FTC has released over time that attempt to explain the test. The test in its current form is vague, and it is applied unpredictably and inconsistently on a case-by-case basis.[149] The following is an explanation of the test as it appears to apply today based upon the limited resources available.

The first prong is that "the ... practice causes or is likely to cause substantial injury to consumers."[150] Most cases will involve monetary harm, but the injury could also be "[u]nwarranted health or safety risks."[151] Emotional harm is never a factor.[152] The question, then, turns on what "substantial injury" means.

---

147. *Compare* 15 U.S.C. § 45(n) (1994), *with id.* (2012) (using identical language).

148. Woods, *supra* note 80.

149. Wright, *supra* note 12, at 5-7, 10.

150. 15 U.S.C. § 45(n) (2012); *see* FTC POLICY STATEMENT ON UNFAIRNESS, *supra* note 44, at app. at 1073.

151. FTC POLICY STATEMENT ON UNFAIRNESS, *supra* note 44, at app. at 1073.

152. *Id.*

In the FTC's 1980 Policy Statement on Unfairness, it stated that a substantial injury does not include harm that is "trivial or merely speculative."[153] Since then, the FTC has continued to argue that an actual breach is not required for the FTC to meet the first prong of the unfairness test.[154]

For example, in *LabMD* the FTC filed a complaint alleging that LabMD violated section 5 of the FTC Act by engaging in unfair acts or practices even though the record contained no evidence of actual injury.[155] The FTC's justification for filing a complaint was that section 5 of the FTC Act allows for a mere "likelihood" of substantial injury and that LabMD's data security practices unfairly exposed consumers' data.[156] Chairwoman Ramirez held in the Opinion of the Commission that the "privacy harm resulting from the unauthorized disclosure of sensitive health or medical information is in and of itself a substantial injury."[157]

Notwithstanding the holding, Chairwoman Ramirez went on to discuss whether there was a substantial likelihood of injury.[158] She stated that Chief ALJ Chappell applied the wrong standard to this question when he held that harm had to be probable, not just possible, in order to be likely.[159] She held instead that harm is likely if there is a "significant risk" of harm, and she repeatedly emphasized that even though the harm may be contained to a small number of consumers, a practice may still be unfair as long as the impact to those consumers is great.[160] Chairwoman Ramirez also noted that subjective harm may be considered in this analysis "in extreme cases."[161]

Despite the final holding in *LabMD*, the future application of the first prong is unclear. The *LabMD* rule applies only to those cases involving "sensitive health or medical information."[162] Any other

153. *Id.*

154. *See, e.g.*, Opposition to Motion to Dismiss, LabMD, Inc., F.T.C. Docket No. 9357, at 3 (June 6, 2014), https://www.ftc.gov/system/files/documents/cases/570399.pdf [https://perma.cc/Z72S-25CL].

155. *See* Initial Decision, LabMD, Inc., *supra* note 100, at 52.

156. *See* Opposition to Motion to Dismiss, LabMD, Inc., *supra* note 154, at 3-7.

157. Opinion of the Commission, LabMD, Inc., *supra* note 29, at 19.

158. *See id.* at 20.

159. *Id.*

160. *Id.* at 10, 20-21.

161. *Id.* at 10.

162. *See id.* at 19.

type of information would be subject to the "significant risk" standard, which is vague and could easily be manipulated by ALJs to mean anything.[163] Also, in cases involving subjective harm, there is no clear understanding of which cases ALJs will consider to be "extreme."[164] But the first prong is not the only vague portion of the unfairness test.

The second prong of the unfairness test is that "the injury must not be outweighed by any offsetting consumer or competitive benefits that the sales practice also produces."[165] In the FTC's 1980 Policy Statement, it recognized that companies make "tradeoffs" for the benefit of business.[166] For example, "[a] seller's failure to present complex technical data on his product may lessen a consumer's ability to choose ... but may also reduce the initial price he must pay for the article."[167] Such tradeoffs include not only burdens to individual consumers, but also burdens to society.[168] The basic requirements are that businesses must supply consumers with sufficient information, and they cannot exert undue influence over the consumers.[169] When considering this prong, the FTC claims it "take[s] into account the cost to remedy the alleged injury to the parties involved, as well as 'the burdens on society in general in the form of increased paperwork, increased regulatory burdens on the flow of information, reduced incentives to innovation and capital formation, and similar matters.'"[170]

---

163. *See id.* at 21 (explaining the "significant risk" standard).

164. *See id.* at 10. Although Chairwoman Ramirez provides "abusive debt collection practices" and "high pressure sales tactics" as examples of "extreme cases" in which subjective harm may be considered by the FTC, they are merely examples that exist in a congressional report and an FTC guidance statement, not examples of subjective harm that have been considered in actual cases. *See id.* (citing S. REP. NO. 103-130, at 13 (1993)). Furthermore, these are only examples that *may* be applied to the unfairness test, not examples that *must* be applied. *See id.* The statement that "subjective types of harm might well be considered as the basis for a finding of unfairness" in "extreme cases" is vague on its face and leaves companies unable to determine the strength of their cases if they choose to challenge the FTC. *See id.*

165. FTC POLICY STATEMENT ON UNFAIRNESS, *supra* note 44, at app. at 1073.

166. *Id.*

167. *Id.*

168. *See id.*

169. *Id.* at app. at 1074.

170. Scott, *supra* note 1, at 159 (quoting FTC POLICY STATEMENT ON UNFAIRNESS, *supra* note 44, at app. at 1073-74).

Exactly how this prong plays out is still largely unknown because the FTC has settled almost all of its data security cases.[171] *Wyndham* and *LabMD* provide little guidance. Because *Wyndham* involved three major breaches and a significant amount of harm, it is unhelpful for understanding how the FTC will apply the second prong to smaller businesses or cases involving minor data security issues.[172]

As for *LabMD*, Chairwoman Ramirez emphasized the existence of relatively low-cost tools that could have been implemented by LabMD, and she balanced that against what she considered to be substantial harm to consumers, ultimately deciding that harm to consumers outweighed the cost to LabMD.[173] She stated that this was a clear case of harm to consumers outweighing the harm to the company, but her reasoning was based on an unprecedented finding: that the release of any medical information through any medium constitutes actual, substantial harm.[174] Moreover, Chairwoman Ramirez's reasoning appeared to be based on the assumption that LabMD should have known that its software was insufficient or that its IT staff did not already have the proper training.[175] The way she applied the first two prongs does make the harm to consumers substantially outweigh any burden on LabMD, but, again, the FTC possesses significant institutional bias,[176] and LabMD can still appeal the final order. Moreover, how the FTC will apply this prong in cases with a mere likelihood of harm, or just a different type of harm, remains a mystery.

The third prong of the unfairness test is that "the injury must be one which consumers could not reasonably have avoided."[177] An injury is reasonably avoidable by consumers when consumers can make their own decisions based on the market.[178] In its 1980 Policy Statement on Unfairness, the FTC emphasized that consumer choice is what governs the market and that this effect should be

171. *See supra* Part II.A.
172. FTC v. Wyndham Worldwide Corp., 799 F.3d 236, 241-42 (3d Cir. 2015).
173. *See* Opinion of the Commission, LabMD, Inc., *supra* note 29, at 26-28.
174. *See id.* at 19, 28.
175. *See id.* at 12-16.
176. *See supra* notes 146-47 and accompanying text.
177. FTC POLICY STATEMENT ON UNFAIRNESS, *supra* note 44, at app. at 1073-74.
178. *Id.*

"self-correcting."[179] If consumers chose not to avoid the injury, then "it would be paternalistic for the FTC to step in and protect them."[180] The FTC should only step in when there is an "obstacle to the free exercise of consumer decisionmaking."[181] This includes certain sales techniques that make consumers unable to fairly consider their options before choosing to participate in the market.[182]

Once again, the FTC has not had much opportunity to apply the third prong in unfairness cases because of the lack of litigation.[183] In *Wyndham*, the argument on prong three revolved around deceptive practices rather than unfair practices, which invoke a different test entirely.[184] *LabMD*, however, provides some minimal level of guidance. In *LabMD*, Chairwoman Ramirez held that "consumers had no ability to avoid the harms caused by LabMD's practices" because the patients were not directly tied to LabMD.[185] Instead, LabMD's clients were the physicians and other health care providers that drew the samples from their patients.[186] The patients could not choose where to send their samples, and they were not "reasonably capable of mitigating any injury 'after the fact'" because LabMD failed to provide them with notice of the breach.[187] What is left unanswered is whether LabMD could have won on the third prong if it had provided notice or if Commissioner Ramirez would have found for LabMD on this issue if the patients themselves chose where to send their samples for testing. Outside of the specific facts of this case, it is difficult to know how the FTC will apply this prong in future cases.

---

179. *Id.*

180. Dennis D. Hirsch, *That's Unfair! Or Is It? Big Data Discrimination and the FTC's Unfairness Authority*, 103 KY. L.J. 345, 354 (2014).

181. FTC POLICY STATEMENT ON UNFAIRNESS, *supra* note 44, at app. at 1074; *see* Beales, *supra* note 6, at 196.

182. *See* FTC POLICY STATEMENT ON UNFAIRNESS, *supra* note 44, at app. at 1074.

183. *See supra* notes 149-50 and accompanying text.

184. FTC v. Wyndham Worldwide Corp., 799 F.3d 236, 245-46 (3d Cir. 2015) ("[C]onsumers could not reasonably avoid injury by booking with another hotel chain because Wyndham had published a misleading privacy policy that overstated its cybersecurity.").

185. Opinion of the Commission, LabMD, Inc., *supra* note 29, at 25.

186. *Id.*

187. *Id.* at 25-26.

III. THE ANTITRUST RULE OF REASON AS A GUIDELINE FOR APPLYING THE UNFAIRNESS TEST

A. The Current Application of the Unfairness Test Harms Competition

The FTC's invasive data security initiatives harm small and independently owned businesses when the FTC fails to adequately tailor its investigation to each company or organization.[188] The initiatives harm these businesses by hindering their ability to successfully compete in the market.[189] Alden Abbott, the former director of antitrust policy for the FTC, argues that "data security investigations that are not tailored to the size and capacity of the [company] may impose competitive disadvantages on smaller rivals in industries in which data protection issues are paramount."[190] This is because larger companies have the ability and resources to support more expensive and invasive provisions in consent decrees.[191] In fact, it may even be in the interest of larger companies to do so. Abbott discusses a concept known as a "raising rivals' costs" strategy, a method of competition whereby larger companies take on costs that would either eliminate smaller companies or substantially harm them in a manner that virtually removes them from competition.[192] In the end, such a strategy harms consumers who must then pay more for goods and services that might be lower in quality.[193]

Hindering the ability of small businesses to successfully compete in the market is particularly harmful to the economy because small businesses contribute to economic growth.[194] Increased regulation harms small businesses because it disproportionately affects them. Commissioner J. Thomas Rosch argues that the FTC's final 2012 Privacy Report "repeatedly sides with consumer organizations and

188. *See, e.g.*, *supra* notes 119-45 and accompanying text.

189. *See supra* notes 139-45 and accompanying text.

190. Abbott, *supra* note 74, at 5.

191. *Id.*

192. *Id.* (quoting David T. Scheffman & Richard S. Higgins, *Twenty Years of Raising Rivals' Costs: History, Assessment, and Future*, 12 GEO. MASON L. REV. 371 (2003)).

193. *Id.*

194. *See* George L. Priest, Essay, *Small Business, Economic Growth, and the Huffman Conjecture*, 7 J. SMALL & EMERGING BUS. L. 1, 2 (2003).

large enterprises."[195] Commissioner Rosch also argues that the FTC should only apply section 5 in cases of "monopoly or near-monopoly power."[196] Otherwise, large companies with such power will use privacy as a "weapon" against other businesses, thereby harming competition.[197] The following Sections provide examples of how the FTC's proposed data security measures harm small companies.

1. The Unfairness Test Is Vague, and the FTC's Current Application of It Is Unpredictable

The FTC currently takes an ad hoc approach in choosing which unfair acts or practices to pursue.[198] This approach is problematic because the unfairness test itself is already "vague and ambiguous," and companies cannot easily anticipate what constitutes a breach.[199] Former Commissioner Wright noted in February 2015 that the FTC failed to commit to a stable definition of what makes particular data security acts or practices unfair.[200] This is the case even though commissioners across the political spectrum agree that a "principled standard" for such would be a "welcome improvement."[201] Even Commissioner Rosch is skeptical of the FTC using the unfairness power in data security cases because of its vagueness and subjectiveness.[202]

Current application of the unfairness test is burdensome to small businesses because businesses can be punished for taking actions they did not know would constitute a breach. This, in turn, hurts the market because businesses cannot stay in the market and help increase competition. Although *Wyndham* is not direct evidence of this conclusion because Wyndham's breach was so egregious, *Wynd-*

195. FED. TRADE COMM'N, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE: RECOMMENDATIONS FOR BUSINESSES AND POLICYMAKERS C-4 (2012) [hereinafter 2012 PRIVACY REPORT] (Rosch, Comm'r, dissenting), https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf [https://perma.cc/YN4F-3839].

196. *Id.* at C-5.

197. *Id.* at C-4 to C-5.

198. *See* Wright, *supra* note 12, at 5.

199. *See id.*

200. *Id.*

201. *Id.*

202. *See* 2012 PRIVACY REPORT, *supra* note 195, at C-3 (Rosch, Comm'r, dissenting) ("'Unfairness' is an elastic and elusive concept. What is 'unfair' is in the eye of the beholder.").

ham provides a helpful framework for understanding how the FTC's ALJs, Commissioners, and other courts may approach the issue of notice. Wyndham argued that the FTC could not file a complaint against it because it was never put on notice.[203] The Third Circuit held that the FTC gave sufficient notice because Wyndham was not entitled to know what the FTC's interpretation of section 5 would be with "ascertainable certainty."[204] Instead, the relevant question was "whether Wyndham had fair notice that its conduct could fall within the meaning of the statute."[205] Wyndham's acts and practices were so extreme that they clearly fell within the fair notice requirement because Wyndham sustained three major breaches in a short amount of time.[206]

LabMD, on the other hand, was found to be engaging in unfair acts or practices for actions that were not so obvious. LabMD had security software on its computers, its employees used passwords, and it had IT staff.[207] The problem, according to Chairwoman Ramirez, was that LabMD did not update its software, routinely run checks to detect vulnerabilities, train its IT staff on data security issues, or train its employees to have better security practices, in-`cluding more secure passwords.[208] Aside from noting that LabMD failed to provide regular data security training to its employees, as set forth in its compliance manual, Chairwoman Ramirez did not appear to even consider whether LabMD was aware that its practices were insufficient.[209] Instead, she placed a great deal of emphasis on the fact that proper security measures could have been implemented with little cost to LabMD.[210] But the mere existence of low-cost security measures does not mean that LabMD should have known of them or was on notice that it should implement those measures. Thus, *LabMD* does not necessarily clear up which acts or practices the FTC will consider "unfair."

The lack of clarity on what constitutes a breach is apparent in other cases as well. In the FTC's case against HTC America, Inc.,

203. *See* FTC v. Wyndham Worldwide Corp., 799 F.3d 236, 249 (3d Cir. 2015).
204. *Id.* at 251.
205. *Id.* at 255.
206. *See id.* at 255-56.
207. Opinion of the Commission, LabMD, Inc., *supra* note 29, at 11-16.
208. *Id.*
209. *See generally id.*
210. *Id.* at 11-16.

the FTC charged HTC with a failure to provide reasonable and appropriate security in the design of its smartphone software.[211] However, the FTC did not cite any specific harmful security breaches to justify such sanctions.[212] The decree did not even explain what specific steps short of the decree requirements would have been deemed "reasonable."[213]

Even the consent decrees do not provide sufficient notice. As stated previously, the consent decrees are all nearly identical.[214] Moreover, the language of the consent decrees provides little guidance because they merely state that the companies should implement "a comprehensive information security program."[215] This does not even inform the companies actually signing the consent decrees of what constitutes adequate security practices.

Without knowing what constitutes unfair security acts or practices, small companies will be blindsided by the FTC, and that itself is unfair.

2. The FTC's Proposed Data Security Measures Are Too Costly with Little Incentive to Challenge Them

The FTC's proposed security measures impose a disproportionately high cost to smaller or independently owned businesses. The actual cost for such security measures varies based on the type of business and the way it is run. One company in Utah gave an estimate of how much a small business should spend on data

---

211. *See* Complaint, HTC Am., Inc., F.T.C. Docket No. C-4406, at 2 (Feb. 22, 2013), https://www.ftc.gov/sites/default/files/documents/cases/2013/07/130702htccmpt.pdf [https://perma.cc/F4ZU-4V8W].

212. Alden Abbott stated,

> The HTC settlement exemplifies the FTC's "security by design" approach to data security. This approach informs firms after the fact what they should have done without exploring what they might have done to pass agency muster. It is inherently vague and puts the FTC in the position of being a "data security systems designer."

Abbott, *supra* note 74, at 4.

213. *Id.*

214. *See supra* notes 94-96 and accompanying text.

215. *See, e.g.*, Final Order, LabMD, Inc., *supra* note 30, at 2; DSW, Inc., 141 F.T.C. 117, 123 (2006) (Decision & Order); BJ's Wholesale Club, Inc., 140 F.T.C. 465, 470-71 (2005) (Decision & Order).

security: roughly "$57,600 a year for a 50-employee company."[216] This includes secure e-mail hosting, an antivirus service, online backup, a secure Internet phone system, and labor costs.[217] Furthermore, each of these is calculated on a per-employee basis.[218] The less tech-savvy a business is, and the more it needs to rely on IT staff or outsourcing, the greater the costs will be.[219]

Most of the consent decrees the FTC issues pose a significant burden on businesses, far beyond what smaller companies can sustain in time, money, and available resources—that is, knowledgeable technology and support staff. The FTC action involving TRENDnet is one example of a disproportionately burdensome consent decree for a problem that the company had seemingly resolved.[220] TRENDnet is a California company that, among other things, sells networking devices to individuals and small- and mid-sized businesses.[221] The *TRENDnet, Inc.*, case involved security cameras the company sold for customers to use inside their houses.[222] In January 2012, hackers invaded 700 customers' security cameras and opened up each of those systems on a live feed.[223] TRENDnet quickly released new software to eliminate the problem, and it encouraged consumers to install the new software.[224] Thereafter, the FTC filed its complaint against TRENDnet.[225] The company argued that it took reasonable steps to ensure its cameras were secure, which the FTC contended was a misrepresentation.[226]

Only a few months later, TRENDnet signed a consent decree in which the company agreed, among other actions, to implement an entirely new security program, acquire outside audits, and notify

---

216. Patrick Clark, *The Bill for Cybersecurity: $57,600 a Year*, BLOOMBERG BUS. (Oct. 31, 2014), http://www.bloomberg.com/bw/articles/2014-10-31/cybersecurity-how-much-should-it-cost-your-small-business [https://perma.cc/TN2L-UXEK].

217. *Id.*

218. *Id.*

219. *Id.*

220. *See* Complaint, TRENDnet, Inc., F.T.C. Docket No. C-4426, at 5 (Jan. 16, 2014), https://www.ftc.gov/system/files/documents/cases/140207trendnetcmpt.pdf [https://perma.cc/UR23-PRK7].

221. *Id.* at 1.

222. *Id.* at 2.

223. *Id.* at 5.

224. *Id.*

225. *Id.* at 1.

226. *Id.* at 6.

customers about these new policies, as well as the company's new software capabilities.[227] TRENDnet also agreed to provide its affected customers with free technical support for the next two years and to acquire biennial third-party assessments of its security measures for the next twenty years.[228]

Although the FTC maintains that it considers the scale and resources of each company when it begins an investigation,[229] it does not appear to do so in practice. Again, the *TRENDnet* consent decree is substantially similar to the other FTC consent decrees.[230] Refer again to the case of *LabMD*. Although LabMD is a small company, the proposed consent decree provided at the outset was substantially similar to those of other, larger companies, like BJ's Wholesale Club.[231] Moreover, the consent decrees and proposed consent decrees in cases involving major breaches are practically identical to those in cases like *LabMD* and *TRENDnet*, in which the companies under investigation had already taken steps to remedy data security problems.[232]

Despite this, small businesses can afford neither to challenge nor concede to these consent decrees. As stated previously, LabMD spent so much money on litigation that it was forced to wind down and eventually end its operations.[233] LabMD expended enormous costs challenging the FTC in a case in which the FTC could show no evidence of patient harm, or that there was even a substantial likelihood of harm.[234] In addition to ceasing its operations, LabMD

227. Decision & Order, TRENDnet, Inc., F.T.C. Docket No. C-4426, at 4-6 (Jan. 16, 2014), https://www.ftc.gov/system/files/documents/cases/140207trendnetdo.pdf [https://perma.cc/83LR-Y74Q].

228. *See id.* at 6-7.

229. *See* 2012 PRIVACY REPORT, *supra* note 195, at 9.

230. *See supra* Part II.A.

231. *See* Abbott, *supra* note 74, at 5. For example, compare Complaint, LabMD, Inc., *supra* note 25, at 7-9, with Decision & Order, TRENDnet, Inc., *supra* note 227, at 4-6.

232. *See* Complaint, TRENDnet, Inc., *supra* note 220, at 5 (identifying that TRENDnet seemingly resolved the problem as soon as it discovered the problem by releasing new software to block hacking); Complaint, LabMD, Inc., *supra* note 25, at 4-5 (identifying that LabMD uninstalled Limewire from the computer as soon as it learned of the breach).

233. *See* Abbott, *supra* note 74, at 5; Epstein, *supra* note 23.

234. *See* Initial Decision, LabMD, Inc., *supra* note 100, at 92.

suffered reputational damage by publicly wrestling with FTC ligigation for six years.[235]

The FTC also fails to take account of the fact that these companies must sustain the additional burdens that state regulations impose. In the realm of data security, many states impose a notice requirement on businesses, whereby, in the event of a breach, businesses must inform each and every customer whose private information is compromised.[236] Whether such state regulations are good or bad, and whether the state should even regulate data security at all, are separate questions entirely. For purposes of this Note, such regulations should be simply viewed as additional burdens which only make the weight of FTC consent decrees that much more difficult for small companies to bear.

Ultimately, businesses have little incentive to challenge the FTC. Even LabMD, which won at the initial stage, lost on appeal at the hands of the FTC's institutional bias.[237] Former Commissioner Wright discussed this bias at the FTC's February 2015 symposium on section 5 of the FTC Act.[238] He argued that one "strong sign of an unhealthy and biased institutional process" is that "in 100 percent of cases where the administrative law judge ruled in favor of the FTC staff, the Commission affirmed liability; and in 100 percent of the cases in which the administrative law judge ... found no liability, the Commission reversed."[239] Former Commissioner Wright also argued that "the combination of institutional and procedural advantages with the vague nature of the Commission's section 5 authority gives the agency the ability, in some cases, to elicit a settlement even though the conduct in question very likely may not be anticompetitive."[240] Those settlements, in turn, perpetuate the process by which the FTC regulates unfair acts or practices because

235. *See* C. Ryan Barber, *Medical Company LabMD Sues FTC Lawyers over Data-Privacy Case*, NAT'L L.J. (Nov. 23, 2015), http://www.nationallawjournal.com/id=1202743147127/Medical-Company-LabMD-Sues-FTC-Lawyers-Over-DataPrivacy-Case?slreturn=20160122150652 [https://perma.cc/TC5N-56BB].

236. *See, e.g.*, CAL. CIV. CODE §§ 1798.29, 1798.82-.83 (West 2017); FLA. STAT. §§ 282.318(3)(i), 501.171(2) (2017); N.Y. GEN. BUS. LAW. § 899-aa (LexisNexis 2017); N.Y. STATE TECH. LAW § 208 (LexisNexis 2017).

237. *See* Final Order, LabMD, Inc., *supra* note 30, at 1.

238. *See* Wright, *supra* note 12, at 6.

239. *Id.*

240. *Id.* at 7.

settlements do not allow for any meaningful discussion on or challenge to the FTC's authority.[241]

3. The FTC's Proposed Data Security Measures Harm Innovation

The FTC's invasive data security measures pose a serious threat to innovation.[242] Threats to innovation, in turn, harm competition, consequently harming consumers.[243] The FTC has set forth a number of policy statements explaining what it deems to constitute good security practices.[244] One of its suggestions is that companies should dispose of private information for which they have no use after a certain period of time.[245] Although the FTC claims that this time limit for disposal is flexible depending on the company, not all of the FTC commissioners are convinced.[246] Commissioner Ohlhausen argued that limiting the use of personal data to each particular task and then disposing of it afterwards would pose a harm to science- and technology-based companies that rely on this information for data collection and research.[247] This is direct evidence that the FTC's regulations simply cannot function as a one-size-fits-all approach.

These proposed measures will harm innovation. To demonstrate, consider companies like TRENDnet, which are involved in what is known as the "Internet-of-Things."[248] The "Internet-of-Things" is "a category of consumer products with their own interconnectivity to the Internet and other electronic devices."[249] With too many

241. *See id.*

242. *See* Abbott, *supra* note 74, at 4.

243. *See* Neil W. Averitt & Robert H. Lande, *Using the "Consumer Choice" Approach to Antitrust Law*, 74 ANTITRUST L.J. 175, 175-78 (2007) (stating that innovation is important to consumers because consumers want options).

244. *See, e.g.*, 2012 PRIVACY REPORT, *supra* note 195, at 28.

245. *Id.*

246. *See, e.g.*, Maureen K. Ohlhausen, Comm'r, Fed. Trade Comm'n, The Power of Data, Remarks at the Georgetown University McCourt School of Public Policy and Georgetown Law Center: Privacy Principles in the Era of Massive Data (Apr. 22, 2014), https://www.ftc.gov/system/files/documents/public_statements/299801/140422georgetownbigdataprivacy.pdf [https://perma.cc/WN7W-YJCZ].

247. *See id.* at 12-13.

248. Abbott, *supra* note 74, at 6.

249. *Id.*

restrictions on what companies can do with private data, not only will companies be disincentivized to develop new "Internet-of-Things" technology, but also they may even be *restricted* from doing so.[250] And these are services consumers desire, especially in today's highly technology-based society.[251] Thus, innovation should be a consideration in the application of the unfairness prongs.[252]

B. A New Framework

The FTC should change the way it applies the second prong of its analysis in order to improve the way it regulates potentially unfair data security acts or practices. Instead of its current practices, the FTC should apply an analysis similar to its Sherman Act of 1890 (Sherman Act) antitrust rule of reason analysis when analyzing the balancing prong of the unfairness test.[253] The Sherman Act makes illegal "[e]very contract, combination in the form of trust or otherwise, or conspiracy, in restraint of trade or commerce among the several States."[254]

The Supreme Court first endorsed the rule of reason as the test for applying section 1 of the Sherman Act in the case of *Standard Oil Co. of New Jersey v. United States*.[255] The content of that test "began to take shape" in *Chicago Board of Trade*, a 1918 case.[256] In that case, Justice Brandeis held that "[t]he true test of legality" is whether the restraint imposed promotes or suppresses competition.[257] According to the Supreme Court, that question requires a

---

250. *See id.*

251. *See id.*

252. Alden Abbott noted:

> Missing from the consent decree calculus is the question of whether the benefits in diminished data security breaches justify those costs—a question that should be at the heart of unfairness analysis. There are no indications that the FTC has even asked this question in fashioning data security consents, let alone made case-specific cost-benefit analyses.

Id. at 4-5.

253. *See, e.g.*, Standard Oil Co. of N.J. v. United States, 221 U.S. 1, 66 (1911).

254. Sherman Act § 1, 15 U.S.C. § 1 (2012).

255. 221 U.S. at 66.

256. Bd. of Trade v. United States, 246 U.S. 231 (1918); *see also* Andrew I. Gavil, *Moving Beyond Caricature and Characeriziation: The Modern Rule of Reason in Practice*, 85 S. CAL. L. REV. 733, 742 (2012).

257. *Bd. of Trade*, 246 U.S. at 238.

consideration of "the facts peculiar to the business to which the restraint is applied; its condition before and after the restraint was imposed; the nature of the restraint and its effect, actual or probable."[258] Justice Brandeis acknowledged that "restraints on competition may often be a valuable and integral part of business arrangements, and that not all restraints should be condemned."[259]

The main purpose for applying a rule of reason analysis is to draw a distinction between anticompetitive acts or practices and conduct that is efficient for businesses.[260] A plaintiff must prove the following three elements to bring a section 1 claim under the Sherman Act: "(1) that there was a contract, combination, or conspiracy; (2) that the agreement unreasonably restrained trade under either a per se rule of illegality or a rule of reason analysis; and (3) that the restraint affected interstate commerce."[261] In sum, "[a] restraint violates the rule of reason if the restraint's harm to competition outweighs its procompetitive effects," which is similar to the balancing prong of the unfairness test.[262]

Under the rule of reason, courts apply a balancing test that involves a burden-shifting framework.[263] First, the plaintiff must show that the restraint has significant anticompetitive effects.[264] Then, if the plaintiff succeeds, the defendant must show the legitimate procompetitive effects of the restraint.[265] Finally, if the defendant succeeds, the burden is shifted back to the plaintiff, who must show that the defendant could meet those objectives through less restrictive means.[266] If the plaintiff meets its burden, then the

---

258. *Id.*

259. Gavil, *supra* note 256, at 742 (citing *Bd. of Trade*, 246 U.S. at 238).

260. By "the new rules of reason," Gavil means the rule of reason as it exists today and not in 1911. *See id.* at 735.

261. Tanaka v. Univ. of S. Cal., 252 F.3d 1059, 1062 (9th Cir. 2001) (quoting Hairston v. Pac. 10 Conference, 101 F.3d 1315, 1318 (9th Cir. 1996)); *accord In re* Ins. Brokerage Antitrust Litig., 618 F.3d 300, 315 (3d Cir. 2010) (requiring the plaintiff to show (1) "that the defendant was a party to a contract, combination ... or conspiracy" and (2) "that the conspiracy to which the defendant was a party imposed an unreasonable restraint on trade" (internal quotation marks omitted) (quoting Toledo Mack Sales & Serv., Inc. v. Mack Trucks, Inc., 530 F.3d 204, 218 (3d Cir. 2008))).

262. *Tanaka*, 252 F.3d at 1063 (citing *Hairston*, 101 F.3d at 1319).

263. *See* O'Bannon v. Nat'l Collegiate Athletic Ass'n, 802 F.3d 1049, 1070 (9th Cir. 2015); *see also In re Ins. Brokerage Antitrust Litig.*, 618 F.3d at 316.

264. *See O'Bannon*, 802 F.3d at 1070.

265. *See id.*

266. *See id.*

plaintiff wins the case.[267] If not, the court steps in and weighs the anticompetitive and procompetitive effects of such a restraint.[268]

When applying this approach to the second prong of the unfairness test, courts should use a similar analysis. First, the FTC must show substantial harm or a likelihood of substantial harm, as evidenced by the *LabMD* analysis above.[269] If the FTC succeeds, then the burden will be on the company to show how the FTC's action against it is actually anticompetitive. This may be shown by (1) providing evidence that the FTC sanction will run the company out of business or severely hamper its ability to conduct business, and (2) providing evidence that the harms to the company will ultimately harm the market by providing consumers with fewer choices. The evidence will include considerations of the cost of implementing more sophisticated data security measures, whether the company remedied any problems, how its practices compare against those of other companies with a similar size and purpose, how an FTC consent order will hinder the company's willingness and ability to innovate, whether the company could have reasonably known that its practices would warrant an FTC action, whether this action would significantly reduce the company's business or shut it down altogether, and other similar concerns. If there is a sufficient finding that the FTC's enforcement action is anticompetitive, then it will be up to the FTC to prove with certainty that the harm to consumers and competition caused by the company's actions are *substantially* more anticompetitive than the FTC's regulation of such actions.

The FTC should conduct this analysis on its own before it decides to even file the complaint. Otherwise, the cost of litigating a weak FTC case will only pose an additional burden on these businesses, which will be especially detrimental if the businesses are smaller. The cost of business practices needs to "clearly outweigh" any benefits before the FTC can go after the business.[270]

---

267. *See* Mass. Bd. of Registration in Optometry, 110 F.T.C. 549, 604 (1988) (Opinion of the Commission); Michael A. Carrier, *The Real Rule of Reason: Bridging the Disconnect*, 1999 BYU L. REV. 1265, 1268.

268. *See Mass. Bd. of Registration in Optometry*, 110 F.T.C. at 604; Carrier, *supra* note 267, at 1268-69.

269. *See* Initial Decision, LabMD, Inc., *supra* note 100, at 92.

270. *See* Abbott, *supra* note 74, at 9.

C. Why This Framework?

As the unfairness test stands today, any cost-benefit analysis engaged in by the FTC is meaningless because the FTC is ignoring key considerations, such as the effect of an enforcement action on the market, which ultimately impacts consumers. Adding the rule of reason analysis to the balancing portion of the unfairness test forces the FTC to at least think about the broader impact of an enforcement action. This is especially important in cases involving potential, rather than actual, harm to consumers.

Additionally, this new emphasis on cost-benefit analysis will provide more clarity for businesses on what the FTC expects out of them.[271] There is not much existing judicial guidance, and the uncertainty businesses face is costly. Uncertainty costs businesses money, time, and resources to implement measures they may or may not need because they are merely guessing. Furthermore, uncertainty costs businesses in innovative abilities.

Even former Commissioner Wright argues that application of the unfairness test necessarily calls for an economic analysis.[272] Such an economic analysis should be flexible, and it should incorporate harms to consumers on the one hand and benefits to consumers and competition on the other.[273] Alden Abbott also argues for an economic analysis here, placing the focus on "marginal benefits" and "marginal costs."[274]

This concept is not so new that it would be shocking for the FTC. It simply forces the FTC to take much more careful consideration of the harms of bringing a data security action. This approach will make the most difference in cases like *LabMD* and *TRENDnet*, in

---

271. *See id.*

272. *See* Joshua D. Wright, Comm'r, Fed. Trade Comm'n, The Economics of Digital Consumer Protection: One Commissioner's View, Remarks at TechFreedom and International Center for Law and Economics (July 31, 2014), https://www.ftc.gov/system/files/documents/public_statements/573061/010731techfreedom.pdf [https://perma.cc/S544-SZ9C].

273. *See id.*

274. Alden Abbott states,

> Economic logic indicates that the optimal business policy is not one that focuses solely on implementing the strongest data protection system program without regard to cost. Rather, the optimal policy is to invest in enhancing corporate data security up to the point where the marginal benefits of additional security equal the marginal costs, and no further.

Abbott, *supra* note 74, at 2.

which it appears that the companies took steps to remedy the harms as soon as they were made aware of them, and in which the alleged violations were minimal.[275]

CONCLUSION

The FTC has overcorrected and overstepped its section 5 unfairness power in data security cases, and it has overcorrected in its efforts to crack down on poor data security practices. In proposing a new framework for cost-benefit analysis, this Note does not argue that there are no data security issues that need to be addressed or that the FTC should stop regulating data security at all. In fact, the FTC should continue to use this power in cases of clear misconduct and egregious acts and practices.[276] But the FTC's enforcement measures go too far. The FTC must begin to limit its reach to only those cases involving serious or obvious misconduct because the burden placed upon smaller or independently owned businesses in cases involving minor violations or only a mere possibility of harm to consumers is far too great. A framework similar to the antitrust rule of reason will help the FTC to filter out these weaker cases, or may even incentivize the FTC to come up with an alternative, less harmful way to handle such cases, such as by creating a system whereby smaller businesses with smaller violations are given a warning with a certain period of time to correct the problem. There are options for enforcement beyond just consent decrees and major investigations.

Applying rule of reason analysis to the balancing portion of the unfairness test will create more stability and predictability. Because weaker cases will be filtered out, the FTC will, in theory, not bring data security cases against businesses that were unaware of a breach in their security because the breach was so minor, or against businesses who were aware a breach occurred but took proper steps to correct it. Those committing serious violations or who were aware

275. *See* Complaint, TRENDnet, Inc., *supra* note 220, at 5; Complaint, LabMD, Inc., *supra* note 25, at 4-5.

276. Alden Abbott also made this argument, citing as support the FTC actions against Credit Karma and Fandango, in which both companies knew about data security problems with their phone applications, but decided to release the applications anyway. *See* Abbott, *supra* note 74, at 6-7.

of a breach but did not do enough to correct it should foresee that they will likely be subject to an FTC investigation. This is a fair way to apply the unfairness test.

Overall, applying rule of reason analysis in these data security cases will benefit both the market and consumers by enabling smaller businesses to continue to successfully compete in the market. They will not be excused from clear cases of misconduct, but those businesses working to protect consumers and correct any errors in data security should not be punished so severely, if at all.

Jennifer L. West[*]

* J.D. Candidate 2017, William & Mary Law School; B.A. 2014, Miami University. I would like to thank my family for always encouraging me in my academic pursuits. Thank you to the staff and editors of the *William & Mary Law Review*, especially Cameron Ginder, for your invaluable feedback and all of the hard work you put into preparing this Note for publication. Finally, thank you to Sean for your patience and support as I poured a great deal of time and energy into this Note.