NOTE

Exposure as Distortion: Deciphering "Substantial Injury" for FTC Data Security Actions

Maxwell E. Loos[*]

ABSTRACT

If the Equifax breach of 2017 demonstrated anything, it is that consumers in the digital age are mostly powerless to protect their sensitive data from hackers and identity thieves—when companies continue to collect massive amounts of sensitive consumer data while failing to invest in appropriate data security measures, consumer welfare will always suffer, and society will always bear a deadweight loss. Since the 1990s, however, the United States Federal Trade Commission has emerged as the "de facto federal data protection authority," protecting consumer welfare under its mandate to prevent "unfair and deceptive acts" in commerce by challenging companies when their unreasonable data security practices unfairly expose sensitive consumer information. Recent litigation, however, has left open the question of whether the FTC may fulfill the statutory "substantial injury" requirement for a successful unfairness claim if it does not allege actual injury to consumers as the result of a particular data exposure.

This Note interprets the language of the "substantial injury" requirement in light of the underlying purposes and design of the FTC Act, arguing that unreasonable exposure of sensitive information can satisfy the requirement even absent a showing of specific harm stemming from the exposure. This is because exposure of sensitive consumer information typically either creates or reflects information asymmetries that reduce consumer welfare, which is exactly the type of harm that the FTC Act was intended to prospectively prevent. To evaluate whether an exposure of consumer information constitutes substantial injury under the FTC Act, courts should utilize a burden-shifting proof structure that considers the sensitivity of the information exposed and the degree of the exposure. This

[*] J.D. 2019, The George Washington University Law School. Deepest thanks for the dedication and insightfulness displayed by every Member, Associate, and Editor of *The George Washington Law Review* on this and on every piece.

formulation would serve the purposes of the FTC Act by prospectively incentivizing the commercial entities that hold large amounts of consumer data to bear the costs of investing in information security, rather than placing the risk and subsequent costs of data breaches on individual consumers.

INTRODUCTION

If the collective shock of the Equifax data breach of 2017[1] was the moment that thrust data security into the collective American consciousness, 2018 was perhaps the year that "opened the eyes of many consumers to the fact that breaches have become 'the new normal.'"[2] While the total number of consumer data breaches reported in 2018 came down[3] from 2017's record-high 1,579,[4] the number of sensitive consumer records exposed more than doubled.[5] The largest single data breach reported in 2018 "exposed information such as passport details, payment card information and date of birth" from 383 million Marriott customers worldwide.[6] Hackers, it would appear, are getting more efficient, at an enormous loss to consumers and to the economy as a whole.[7]

Consumers cannot fully protect their data and their identities on their own. As digital data collection becomes an increasingly ubiquitous feature of commerce in the United States, the consumers whose data is collected need to be confident that it is reasonably safe. The alternative is an economy that forces consumers to bear increased risk of suffering the devastating consequences of identity theft, bear the full costs of data risk mitigation despite being ill-suited to do so, or forsake the advantages of the digital economy entirely. None of these is a particularly appealing option.

Over the past two decades, the Federal Trade Commission has emerged in the United States as the "de facto federal data protection authority."[8] It has

---

1 *See generally* Gillian B. White, *A Cybersecurity Breach at Equifax Left Pretty Much Everyone's Financial Data Vulnerable*, THE ATLANTIC (Sept. 7, 2017, 8:15 PM), https://www.theatlantic.com/business/archive/2017/09/equifax-cybersecurity-breach/539178/ [https://perma.cc/8R57-ZXRM].

2 IDENTITY THEFT RES. CTR., 2018 END-OF-YEAR DATA BREACH REPORT, LESSONS LEARNED FROM 2018 (2019).

3 *Id.* at Key Finding #1.

4 IDENTITY THEFT RES. CTR., 2017 ANNUAL DATA BREACH YEAR-END REVIEW 3 (2018).

5 IDENTITY THEFT RESOURCE CENTER, *supra* note 2, at Key Finding #1.

6 *Id.* at Travel and Your Data.

7 *See* COUNCIL OF ECON. ADVISERS, THE COST OF MALICIOUS CYBER ACTIVITY TO THE U.S. ECONOMY 1 (2018) ("We estimate that malicious cyber activity cost the U.S. economy between $57 billion and $109 billion in 2016.").

8 Daniel J. Solove & Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, 114 COLUM. L. REV. 583, 600 (2014).

done so under its authority to enforce Section 5 of the Federal Trade Commission Act ("Section 5"),[9] which prohibits "unfair or deceptive acts or practices in or affecting commerce."[10] This broad mandate has allowed the Commission to develop something of a "common law" of data protection in the absence of a general data protection statute in the U.S.[11] The FTC's authority to police unreasonably lax data protection practices as unfair, however, has recently been met with resistance: industry groups[12] and defendants[13] have argued that, in order to satisfy the "substantial injury" requirement of an unfairness claim under Section 5(n) of the FTC Act,[14] the FTC must prove that specific harms to consumers have resulted from a data breach. At least one court has agreed.[15]

This Note addresses the statutory "substantial injury" requirement in FTC unfairness claims by focusing on the purposes of the FTC Act, arguing that in an unfairness claim based on unreasonable exposure of consumer data, the FTC may satisfy the substantial injury requirement without alleging specific harms to consumers from the exposure.[16] It reaches this conclusion by situating the FTC's consumer protection mission within the broader context of consumer law, examining the economic purposes and the preventative design of the FTC Act. Part I examines the history of the FTC Act and the development of its unfairness doctrines over the better part of a century. Part I also charts the FTC's entry into the realm of privacy and data security, and then surveys the recent challenges to the Commission's ability

---

9 Federal Trade Commission Act § 5, 15 U.S.C. § 45 (2018).

10 *Id.* § 45(a).

11 *See generally* Solove & Hartzog, *supra* note 8.

12 *See, e.g.*, Glenn G. Lammie & Cory L. Andrews, Comments of Washington Legal Foundation to the Federal Trade Commission Concerning Informational Injury Workshop (Oct. 27, 2017), https://www.ftc.gov/system/files/documents/public_comments/2017/10/00026-141554.pdf [https://perma.cc/4XZ6-ZLLS].

13 Reply Brief of Petitioner, LabMD, Inc., at 3–6, LabMD Inc. v. FTC, 894 F.3d 1221 (11th Cir. 2017) (No. 16-16270).

14 15 U.S.C. § 45(n).

15 *See* FTC v. D-Link Sys., Inc., No. 3:17-cv-00039-JD, 2017 WL 4150873, at *5–6 (N.D. Cal., Sept. 19, 2017).

16 This Note recognizes that Senator Ron Wyden has recently released a "discussion draft" of a privacy bill that would alter Section 5 of the FTC Act such that "substantial injury" would include "those involving noneconomic impacts and those creating a significant risk of unjustified exposure of personal information." Consumer Data Protection Act, S.___, 115th Cong. § 3 (2018) (discussion draft), https://www.wyden.senate.gov/imo/media/doc/Wyden%20Privacy%20Bill%20Discussion%20Draft%20Nov%201.pdf [https://perma.cc/95DK-J93A]. While this would certainly clarify the ambiguity that this Note addresses, the point of this Note is that such a statutory amendment is unnecessary. *See infra* Part III. This Note also goes further than the proposed Section 5 amendment by providing a structure by which courts can determine whether particular conduct has, in fact, amounted to the kind of injury required for a finding of an unfair act or practice in violation of Section 5. *See infra* Part IV.

to prove the "substantial injury" element of an unfairness claim without a showing of actual harm to consumers resulting from a data exposure. Part II highlights the underlying economic purposes and preventative design of Section 5's consumer protection provisions. Part III interprets the language of the "substantial injury" requirement in light of the underlying purposes of the FTC Act—it argues that "substantial injury" occurs for the purpose of Section 5 when information asymmetries in the marketplace are likely to lead to reductions in consumer welfare, and that such a situation occurs when consumer data is exposed due to unreasonable data security practices. Finally, Part IV proposes a burden-shifting proof structure that courts and the Commission can use for determining whether a data exposure constitutes a "substantial injury," focusing on the type of data exposed and the degree of the exposure.

I. THE HISTORY AND PURPOSES OF SECTION 5 OF THE FTC ACT AND THE SUBSTANTIAL INJURY REQUIREMENT

The Federal Trade Commission has been regulating privacy and data security for less than two decades, but it has been regulating competition and protecting consumers for more than 100 years.[17] Determining whether conduct falls under the FTC's authority to prevent unfair practices first requires careful examination of the early history of the FTC's enforcement powers, the modern contours of its unfairness authority, and the questions that have arisen from the FTC's move into the realm of privacy and data security.

A. History of the FTC Act and the Development of Unfairness

The Federal Trade Commission's authority to police data security practices derives from Section 5 of the FTC Act,[18] which prohibits "unfair or deceptive acts or practices in or affecting commerce."[19] The meaning of this broad mandate has evolved over the past century through actions of Congress, of courts, and of the Commission itself, and the meaning of "unfairness" under the statute has developed into a coherent doctrine. This section briefly traces the origins and development of the FTC's unfairness authority under Section 5, as well as the emergence of discrete elements of an unfairness claim in the 1980s and 1990s.

---

17 *See generally* J. Howard Beales III & Timothy J. Muris, *FTC Consumer Protection at 100: 1970s Redux or Protecting Markets to Protect Consumers?*, 83 GEO. WASH. L. REV. 2157, 2157, 2211 (2015).

18 15 U.S.C. § 45 (2018).

19 *Id.* § 45(a)(1).

1. Initial Passage of the FTC Act and the Wheeler-Lea Amendments

Congress passed the FTC Act in 1914 amid widespread concerns about corporate "bigness" and the effects of monopolies and trusts on competition and consumers.[20] There was a perception that the Sherman Antitrust Act[21] had not slowed the pace of industry consolidation,[22] and after the Supreme Court held in *Standard Oil Co. of New Jersey v. United States*[23] that the Sherman Act's prohibition on "every . . . restraint of trade"[24] applied only to "unreasonable" restraints of trade, both business interests and antimonopoly advocates were left in search of new regulatory approaches to the antitrust problem.[25] In response, Congress in 1914 enacted the Federal Trade Commission Act,[26] which broadly prohibited "unfair methods of competition."[27]

Through the 1920s, the FTC used its initial Section 5 authority to prevent false and deceptive advertising, often arguing that deceptive advertising hindered competition by unfairly disadvantaging sellers who advertised products honestly.[28] Many of these were, in essence, consumer protection cases[29] in the garb of a competition mission, and "[b]y 1925, roughly seventy percent of the FTC's orders involved deceptive advertising."[30] The Commission's early foray into consumer protection was halted, however, by the Supreme Court's 1931 decision in *FTC v. Raladam Co.*[31] In *Raladam Co.*, the Commission challenged plainly false claims made by a diet pill manufacturer as unfair methods of competition.[32] The Supreme Court rejected the FTC's assertion that the false claims amounted to an unfair method of competition, however, because while the Commission had presented evidence that the practices could be harmful to purchasers of the pills, it had failed to demonstrate that the deception had harmed competition

---

20 *See* CHRIS JAY HOOFNAGLE, FEDERAL TRADE COMMISSION PRIVACY LAW AND POLICY 3–4 (2015).

21 15 U.S.C. §§ 1–7 (2018).

22 *See* HOOFNAGLE, *supra* note 20, at 5.

23 221 U.S. 1 (1911).

24 15 U.S.C. § 1.

25 *See* HOOFNAGLE, *supra* note 20, at 5–8.

26 Federal Trade Commission Act, Pub. L. No. 63-203, 38 Stat. 717 (1914).

27 *Id.* § 5; *see also* Maureen K. Ohlhausen, *Weigh the Label, Not the Tractor: What Goes on the Scale in an FTC Unfairness Cost-Benefit Analysis?*, 83 GEO. WASH. L. REV. 1999, 2002 (2015).

28 *See, e.g.*, FTC v. Winsted Hosiery Co., 258 U.S. 483, 494 (1922); *see also* Ohlhausen, *supra* note 27, at 2002.

29 *See* Ohlhausen, *supra* note 27, at 2002.

30 *Id.*

31 283 U.S. 643 (1931).

32 *See id.* at 644–45.

by actually diverting business from any competitors.[33] The Court noted that if the FTC was to have authority to prevent injury to consumers, and not just to competition, Congress would need to grant it such authority.[34]

Congress accepted the Supreme Court's invitation to expand the authority of the FTC with the 1938 enactment of the Wheeler-Lea Amendments to the FTC Act.[35] The amended language of Section 5 provided that "[u]nfair methods of competition in commerce, *and unfair or deceptive acts or practices in commerce*, are hereby declared unlawful."[36] The FTC was thus empowered to take action against unfair and deceptive acts regardless of their impact on competition.[37] In a particularly telling demonstration of the change to the FTC's authority, the Supreme Court upheld a second, nearly identical action by the FTC against Raladam,[38] thus confirming the Commission's authority to correct structural market problems when such distortions were preventing consumers from making effective and efficient choices.

2. *The Modern Unfairness Standard: The 1980 Unfairness Statement,* International Harvester*, and the 1994 Amendments*

The FTC largely failed to articulate a cohesive standard for the meaning of unfairness in the years following the Wheeler-Lea Amendments, and it often deemed practices "deceptive and unfair" without distinguishing between the two.[39] By the early 1970s, the Commission had at least determined that, in a pure unfairness analysis without a dimension of deception, it would consider "(1) whether the practice injures consumers; (2) whether it violates established public policy; [and] (3) whether it is unethical or unscrupulous."[40] This was a remarkably broad standard, but one that the Supreme Court seemingly cited with approval.[41] However, facing

---

33 *See id.* at 645, 651–54.

34 *See id.* at 649.

35 Wheeler-Lea Act of 1938, Pub. L. No. 75-447, 52 Stat. 111.

36 *Id.* (emphasis added).

37 *See* HOOFNAGLE, *supra* note 20, at 37 ("Wheeler wanted to reverse the *Raladam* limitation on the FTC, thus allowing the Agency to police deception of the public without explicit evidence of harm to competitors.").

38 *See* FTC v. Raladam Co., 316 U.S. 149 (1942).

39 *See* Ohlhausen, *supra* note 27, at 2003–04.

40 FED. TRADE COMM'N, COMMISSION STATEMENT OF POLICY ON THE SCOPE OF THE CONSUMER UNFAIRNESS JURISDICTION (1980), *reprinted in In re* Int'l Harvester Co., 104 F.T.C. 949, 1072–76 (1984) [hereinafter UNFAIRNESS STATEMENT].

41 *See* FTC v. Sperry & Hutchinson Co., 405 U.S. 233, 244 & n.5 (1972) (citing Statement of Basis and Purpose of Trade Regulation Rule, Unfair or Deceptive Advertising and Labeling of Cigarettes in Relation to the Health Hazards of Smoking, 29 Fed. Reg. 8,324, 8,355 (1964)).

public and political backlash after a failed attempt to regulate children's advertising in the late 1970s[42]—an incident that led the Washington Post to give the FTC the dubious title of "National Nanny"[43]—the Commission in 1980 issued a policy statement articulating a structured interpretation of the meaning of unfairness under the FTC Act.[44] The Commission's seminal application of the new unfairness standard then came in its 1984 opinion in *In re International Harvester Co.*,[45] discussed below, which still serves today as the touchstone of discussions of the FTC's unfairness authority.[46] Finally, in 1994, Congress amended the FTC Act to codify the elements articulated in the FTC's 1980 Unfairness Statement.[47]

a. The FTC's 1980 "Unfairness Statement"

The modern unfairness regime originated in 1980 with the Commission's adoption of the FTC Policy Statement on Unfairness.[48] The FTC adopted the statement after facing withering criticism of its attempts to regulate advertising to children in the 1970's.[49] The statement retreated from previous positions that conduct would be unfair if it violated public policy,[50] or if it were "immoral, unethical, oppressive, or unscrupulous."[51] Rather, the Commission placed consumer injury at the center of its unfairness analysis, stating that "[u]njustified consumer injury is the primary focus of the FTC Act" and "[b]y itself it can be sufficient to warrant a finding of unfairness."[52] The Commission explained, though, that not all consumer injuries would necessitate a finding of unfairness: "To justify a finding of unfairness the injury must satisfy three tests. It must be substantial; it must not be outweighed by any countervailing benefits to consumers or competition that

42 *See* 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, 192–93 (2003).

43 *The FTC as National Nanny*, WASH. POST, Mar. 1, 1978, at A22.

44 *See* UNFAIRNESS STATEMENT, *supra* note 40.

45 104 F.T.C. 949 (1984).

46 *See, e.g.*, Ohlhausen, *supra* note 27, at 2008–09; Joshua D. Wright & John Yun, *Stop Chug-a-lug-a-lugin 5 Miles an Hour on Your International Harvester: How Modern Economics Brings the FTC's Unfairness Analysis Up to Speed with Digital Platforms*, 83 GEO. WASH. L. REV. 2130, 2148–49 n.84, 2156 (2015).

47 *See* Federal Trade Commission Act Amendments of 1994, Pub. L. No. 103-312, § 9, 108 Stat. 1691, 1695 (codified at 15 U.S.C. § 45(n) (2018)).

48 UNFAIRNESS STATEMENT, *supra* note 40.

49 *See* HOOFNAGLE, *supra* note 20, at 60–66.

50 UNFAIRNESS STATEMENT, *supra* note 40, at 1074–76.

51 *Id.* at 1076.

52 *Id.* at 1073.

the practice produces; and it must be an injury that consumers themselves could not reasonably have avoided."[53]

Elaborating on the substantiality requirement, the Commission stated that monetary harms, as well as "[u]nwarranted health and safety risks," would most commonly qualify as substantial.[54] The Commission also explicitly stated that it was "not concerned with trivial or merely speculative harms," including emotional impact.[55] The Commission qualified this contention in a footnote, though, stating that "[a]n injury may be sufficiently substantial, however, if it does a small harm to a large number of people, or if it raises a significant risk of concrete harm."[56] Courts at the time cited this footnote, as well as the Unfairness Statement in general, in determining whether the FTC had proven unfair conduct in violation of Section 5.[57] In *Orkin Exterminating Co. v. FTC*,[58] for example, while the defendant's decision to unilaterally terminate several thousand pest control contracts with consumers did not result in large losses to each individual consumer, the conduct did qualify as an unfair practice based on the large number of consumers affected and the correspondingly large amount of unwarranted revenues collected by the defendant in the aggregate.[59]

b. The FTC's 1984 Decision in International Harvester

The definitive application of the Unfairness Statement's three-part test came with the Commission's 1984 *International Harvester*[60] decision. As former FTC Acting Chair Maureen Ohlhausen notes, "the Commission considered it such a foundational case that they attached the Unfairness Statement to the decision."[61] In *International Harvester*, the FTC examined a line of tractors that had a fuel-geysering problem in which removal of the gas cap could result in an eruption of hot fuel and flame, with the potential to kill or maim the operator.[62] The FTC alleged that the manufacturer's decision not to place a warning label on the tractor, despite its knowledge of

53 *Id.* The second two elements are mostly beyond the scope of this Note, but will be occasionally referred to insofar as they shed light on the meaning of the substantial injury element.

54 *Id.*

55 *Id.*

56 *Id.* at 1073 n.12.

57 *See, e.g.*, Orkin Exterminating Co. v. FTC, 849 F.2d 1354, 1365 (11th Cir. 1988); Am. Fin. Servs. Ass'n v. FTC, 767 F.2d 957, 972–73 (D.C. Cir. 1985).

58 849 F.2d 1354 (11th Cir. 1988).

59 *Id.* at 1355–56, 1365.

60 104 F.T.C. 949, 1060–61 (1984).

61 Ohlhausen, *supra* note 27, at 2006–07.

62 *In re* Int'l Harvester Co., 104 F.T.C. at 950.

the fuel-geysering problem, was an unfair practice.[63] In determining the substantiality of the injuries to consumers, the Commission noted that out of roughly 1.3 million tractors sold, "twelve are known to have been involved in geysering accidents involving bodily injury. This is an accident rate of less than .001 percent, over a period of more than 40 years."[64] Still, the Commission considered the injuries substantial enough to warrant a finding of unfairness given the severity of the physical injuries.[65] Thus, just as a small injury to a large number of consumers could qualify as substantial,[66] a large injury to a small number of consumers would do so as well. The Commission addressed the other two elements articulated in the Unfairness Statement, finding that the risk of injury was "unavoidable" to consumers who had no knowledge of the fuel-geysering issue,[67] and that any price savings passed on to consumers by the company's failure to warn did not outweigh the costs to the consumers injured.[68]

c. Congress's 1994 Addition of Section 5(n)

Finally, in 1994, Congress amended the FTC Act again to codify the Unfairness Statement into necessary elements of an FTC unfairness claim.[69] The amendments added Section 5(n), which states:

> 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.[70]

While the amendment was part of a fairly unheralded procedural bill to grant congressional reauthorization to the FTC,[71] the legislative history

---

63 *Id.* at 1050–51; *see also* Ohlhausen, *supra* note 27, at 2008–09.

64 *Int'l Harvester*, 104 F.T.C. at 1063; *see also* Ohlhausen, *supra* note 27, at 2008.

65 *Int'l Harvester*, 104 F.T.C. at 1064.

66 UNFAIRNESS STATEMENT, *supra* note 40, at 1073 n.12.

67 *Int'l Harvester*, 104 F.T.C. at 1065–66.

68 *Id.* at 1064–65.

69 *See* Federal Trade Commission Act Amendments of 1994, Pub. L. No. 103-312, § 9, 108 Stat. 1691, 1695 (codified at 15 U.S.C. § 45(n) (2018)).

70 15 U.S.C. § 45(n).

71 *See* H.R. 2243, 103d Cong. (1994).

indicated that the goal was explicitly to "provide a strong bulwark against potential abuses of the unfairness standard"[72] and to more clearly define the FTC's "invaluable role in promoting the efficient functioning of our free market economy."[73] The amendment did so by essentially codifying the elements of consumer injury enumerated in the 1980 Unfairness Statement, but crucially, the amended statute deviated from the Unfairness Statement by allowing that an element of an unfair practice is that it "causes *or is likely to cause* substantial injury to consumers."[74]

B. The FTC's Expansion into Data Security and the "Substantial Injury" Question

Of course, exploding toasters and fuel-geysering tractors are not the only threats to consumer welfare in the digital age. In today's era of internet commerce, big data, and increasing reliance on credit cards and other new "fintech," the FTC functions as the "de facto federal data protection authority."[75] When the Commission first stepped into this role around the turn of the century, it relied primarily on deception theories to protect consumer privacy and data security. As its case-by-case approach coalesced to reveal a set of standard data security principles for entities to implement, the Commission began treating unreasonable departures from these principles as unfair practices. Recently, however, there have been several challenges to such actions by the FTC, with defendants arguing (and at least one court agreeing)[76] that in an unfairness action based on an exposure of consumer data, the FTC cannot prove "substantial injury" if it does not show actual, completed harms to consumers from the exposure.

1. The FTC's Entry into Privacy and Data Security

The FTC's first forays into the realms of privacy and data protection enforcement came in the 1990's, as the Commission was charged with enforcing statutory privacy protections[77] such as the Gramm-Leach-Bliley Act[78] and the Children's Online Privacy Protection Act,[79] in addition to enforcing the Fair Credit Reporting Act.[80] The FTC's first data security case

---

72 140 CONG. REC. 17,843 (1994) (statement of Rep. Moorhead).

73 *Id.* at 17,844 (statement of Rep. Manton).

74 15 U.S.C. § 45(n) (emphasis added); *see also infra* text accompanying notes 181–182.

75 Solove & Hartzog, *supra* note 8, at 600.

76 *See infra* Section I.B.2.c.

77 *Id.* at 602–03.

78 Pub. L. No. 106-102, 113 Stat. 1338 (1999).

79 15 U.S.C. §§ 6501–6506 (2018)).

80 15 U.S.C. § 1681 (2018).

came in 2002, when the Commission brought an action against drug manufacturer Eli Lilly, alleging that the company's failure to implement basic security practices led to the disclosure of the email addresses and identities of Prozac users.[81]

When it first began to police privacy and data protection in the earlier days of the internet, the FTC relied primarily on its deception authority under Section 5,[82] as opposed to on its unfairness authority, partially out of concern that the unfairness theory was not well suited for the online realm.[83] The FTC has primarily found acts to be deceptive with regard to privacy and data when a company has made some kind of representation or promise regarding customer privacy or data, and has then broken that promise.[84] The Eli Lilly case, for example, was brought based on representations that the company made in its privacy policy about its data security practices.[85] The FTC has relied heavily on deceptive representations made in privacy policies when bringing privacy and data security actions.[86] And while unfairness claims had appeared in FTC complaints, as in the Commission's case against Facebook,[87] they had often been buoyed by more robust deception claims.[88] Reliance on the deception theory has a flaw, though: it requires a representation to be made to the consumer.[89] This requirement has led the FTC, when faced with obvious consumer injury, to search for some kind of promise made to the consumer that it can claim was broken,[90] a prospect that proves more and more difficult as the Commission seeks to protect

---

81 *In re* Eli Lilly & Co., 133 F.T.C. 763, 767–68 (2002); *see also In re* LabMD, Inc., No. 9357, at 18 (F.T.C. July 29, 2016) (Public Opinion of the Commission).

82 *See* Solove & Hartzog, *supra* note 8, at 628–30.

83 HOOFNAGLE, *supra* note 20, at 156–57. In the 1990s, FTC staff worried that "[online] abuses could be avoided by simply not using the internet as a commercial channel," thus failing the unavoidability element of unfairness. *Id.* at 157. In its first days of online privacy enforcement, when its authority was still somewhat uncertain, the Commission deliberately chose cases with favorable facts, which typically included deception cases involving children's privacy. *Id.*

84 Solove & Hartzog, *supra* note 8, at 628–30. It is worth noting here that an act is deceptive under the FTC Act if it is likely to mislead a consumer who is acting reasonably under the circumstances, and the representation or omission would be material to the consumer. *See* FED. TRADE COMM'N, FTC POLICY STATEMENT ON DECEPTION (Oct. 14, 1983), https://www.ftc.gov/system/files/documents/public_statements/410531/831014 deceptionstmt.pdf [https://perma.cc/5FFD-62YT] [hereinafter DECEPTION STATEMENT].

85 *Eli Lilly*, 133 F.T.C. at 767.

86 *See* Solove & Hartzog, *supra* note 8, at 635–38.

87 Complaint at 7–9, *In re* Facebook, Inc., No. C-4365 (F.T.C. July 27, 2012) (alleging one unfairness count).

88 *Id.* at 4–19 (alleging eight counts of deception).

89 *See* HOOFNAGLE, *supra* note 20, at 346.

90 *See id.*

consumers' sensitive data outside the purely online realm.[91]

After more than a decade of bringing privacy and data security cases, the FTC's case-by-case approach has coalesced into a set of data security principles.[92] On the occasion of its 50th data security case in 2014, the Commission issued a policy statement explaining that:

> The touchstone of the Commission's approach to data security is reasonableness: a company's data security measures must be reasonable and appropriate in light of the sensitivity and volume of consumer information it holds, the size and complexity of its business, and the cost of available tools to improve security and reduce vulnerabilities.[93]

In 2015, the FTC issued guidance to businesses, laying out ten general security practices that the Commission considers reasonably adequate to protect consumer data.[94] The flip side of the reasonability standard is that, if an entity's data security practices do not, as a whole, add up to reasonable protections, the FTC will likely consider this a violation of Section 5.[95] Even without a misrepresentation to a consumer, the FTC has become more willing to bring pure unfairness actions to enjoin unreasonable data security practices—what the FTC must prove in order to satisfy the substantial injury requirement of an unfairness action based on exposure of consumer data, however, has become an open question, as demonstrated in recent litigation.

2. Recent Litigation of the Substantial Injury Requirement in Data Security Cases

While the FTC's common reliance on consent decrees has been criticized for not producing case law for industry to rely on,[96] several recent

---

91 *See* Complaint at 7–8, FTC v. D-Link Corp., No. 3:17-CV-00039-JD (N.D. Cal. Mar. 20, 2017) (alleging that the word "secure" on the box of a wi-fi adapter represented to consumers that the product would be reasonably protected from hacking attacks).

92 Solove & Hartzog, *supra* note 8, at 649.

93 FED. TRADE COMM'N, COMMISSION STATEMENT MARKING THE FTC'S 50TH DATA SECURITY SETTLEMENT 1 (Jan. 31, 2014) https://www.ftc.gov/system/files/documents/cases/140131gmrstatement.pdf [https://perma.cc/Z8WB-YJJP].

94 *See* FED. TRADE COMM'N, START WITH SECURITY: A GUIDE FOR BUSINESS (2015). Each practice is neatly laid out in a chapter title: "Start with security," "Control access to data sensibly," "Require secure passwords and authentication," "Store sensitive personal information securely and protect it during transmission," "Segment your network and monitor who's trying to get in and out," "Secure remote access to your network," "Apply sound security practices when developing new products," "Make sure your service providers implement reasonable security measures," "Put procedures in place to keep your security current and address vulnerabilities that may arise," and "Secure paper, physical media, and devices." *Id.*

95 Solove & Hartzog, *supra* note 8, at 649–50.

96 *Id.* at 606–07.

cases have been litigated, and have raised questions about what should constitute substantial injury in a data security case based on an unfairness theory.

a. FTC v. Wyndham Worldwide*: The Third Circuit Confirms that Data Security Practices Fall Under the FTC's Unfairness Authority*

The FTC made high-profile use of its unfairness authority in a data security action with *FTC v. Wyndham Worldwide*.[97] In *Wyndham*, the FTC challenged the hotel operator's overall lack of data security as an unfair practice under the FTC Act.[98] Among the most egregious practices that the FTC challenged were the storage of payment card information in plain text,[99] the use of default passwords for access to company network systems,[100] failure to implement simple firewalls,[101] failure to update software widely known to be vulnerable,[102] and failure to employ reasonable measures for detecting system intrusions.[103] As a result, the company's network suffered three separate breaches, all using similar methods that could have been thwarted had the company undertaken proper investigation and response.[104] Ultimately, the hackers gained access to the payment card information of more than 619,000 customers, and the FTC alleged at least $10.6 million in losses to consumers, in addition to costs suffered by consumers in mitigating the impact of the theft.[105]

On interlocutory appeal of the district court's denial of Wyndham's motion to dismiss for failure to state a claim, Wyndham argued that its conduct fell outside of the plain meaning of "unfairness,"[106] claiming that because data thieves were the most proximate cause of the actual consumer harms, Wyndham itself could not have unfairly caused any substantial injury to consumers.[107] The court rejected this argument and affirmed that the company's data security practices did fall within the FTC's unfairness

97 799 F.3d 236 (3d Cir. 2015).

98 *See id.* at 240.

99 *See id.*

100 *See id.*

101 *See id.* at 241.

102 *See id.*

103 *See id.*

104 *See id.* at 241–42.

105 *See id.* at 242.

106 *See id.* at 244.

107 *See id.* at 246. Wyndham also argued that specific congressional action on cybersecurity had removed the issue from Section 5's reach, *see id.* at 247, and that the company did not have fair notice of the cybersecurity standards required by Section 5. *See id.* at 249. These contentions are less relevant to the analysis in this Note, but the court ultimately rejected all of Wyndham's arguments. *See id.* at 259.

authority, noting that even if it accepted Wyndham's loose conception of proximate cause, "the FTC Act expressly contemplates the possibility that conduct can be unfair before actual injury occurs."[108] In other words, the company's lax data security practices, by exposing consumers to such a heightened risk of harms like identity theft, constituted an unfair practice even before any hackers stole the data.[109]

With the decision in the Third Circuit, the FTC served notice to the public and to industry that it was ready to challenge failures to use reasonable data security practices to safeguard consumer data, regardless of any representations that the holders of such data may make to consumers. In many ways, *Wyndham* may have been the perfect vehicle for the FTC to assert the application of unfairness to the realm of data security—Wyndham's security practices were so clearly outside the range of reasonability, and the scope of the actual harm to consumers was so massive, that the court had no issue affirming that substantial injury to consumers had occurred as required by Section 5(n). Whether the FTC could satisfy the substantial injury requirement without such a strong showing of completed harms to consumers, however, would prove a more difficult question.

b. LabMD v. FTC*: Opening the Question of Unfairness Claims in the Absence of Actual Consumer Harm*

This more difficult question of whether the FTC could pursue an unfairness claim for a data breach in the absence of a showing of actual consumer harm arose in its *LabMD, Inc.*[110] action. In *LabMD*, the FTC challenged the lax data security practices of a medical testing services company as unfair under Section 5.[111] Specifically, the Commission challenged the company's failure to implement any data security training for its employees for a number of years, as well as the use of default passwords for employee logins.[112] Several employees used LimeWire peer-to-peer software on computers connected to LabMD's servers, and a list of about 9,300 people's names, birth dates, Social Security numbers, medical histories, and other information was discoverable on LimeWire's peer-to-

108 *See id.* at 246. Wyndham additionally raised a *reductio ad absurdum* argument that finding its conduct unfair would lead to the ridiculous result of allowing the FTC to regulate the locks on hotel rooms and sue grocery stores for leaving banana peels on the floor. *See id*. The court responded with "the tart retort that, were Wyndham a supermarket, leaving so many banana peels all over the place that 619,000 customers fall hardly suggests it should be immune from liability under § 45(a)." *Id.* at 247.

109 *See id.* at 246.

110 *In re* LabMD, Inc., No. 9357 (F.T.C. July 29, 2016) (Public Opinion of the Commission).

111 *See id.* at 1, 2.

112 *See id.* at 2.

peer network for several months.[113] Other sensitive data held by LabMD was also found in the possession of identity thieves in an unrelated action, but the FTC did not allege any instances of actual identity theft or medical identity theft from the exposure.[114]

The Commission overturned the initial decision by an Administrative Law Judge that no substantial injury had been proven.[115] First, the Commission found that exposure of sensitive medical information to an unknown party on its own constituted substantial injury.[116] The Commission also found that placement of data on LimeWire was sufficiently likely to cause substantial injury to constitute an unfair act or practice.[117] LabMD appealed the decision to the Eleventh Circuit, which heard arguments on the case in June 2017.[118]

An entire year passed before the Eleventh Circuit released its *LabMD, Inc. v. FTC*[119] ruling in June 2018, and the court ultimately side-stepped the substantial injury question. Rather than rule on the statutory substance of the claim, the court opted instead to rule against the FTC on the basis that the injunction requested was not specific enough to be enforceable.[120] In essence, rather than directly addressing the burning question of whether, in an unfairness action based on exposure of consumer data, the FTC can satisfy the substantial injury requirement of Section 5(n) without alleging specific instances of actual harm to consumers—a question that was extensively briefed by both parties[121]—the *LabMD* court punted.[122] An actual ruling would have added much-needed clarity for both the FTC and industry on a current void in the Section 5 jurisprudence, but for now, the void remains in force.

---

113 *See id.* at 3.

114 *See id.* at 4, 35–36.

115 *See id.* at 7, 25.

116 *See id.* at 17–19.

117 *See id.* at 20–25.

118 *See* Oral Argument, LabMD, Inc. v. FTC, 894 F.3d 1221 (11th Cir. 2018) (No. 16-16270), *available at* http://www.ca11.uscourts.gov/oral-argument-recordings [https://perma.cc/A4ZB-CT6N] (search in case name field for "labmd").

119 894 F.3d 1221 (11th Cir. 2018).

120 *See id.* at 1235–37.

121 *See* Brief of the Federal Trade Commission at 23–30, *LabMD*, 894 F.3d 1221 (No. 16-16270); Reply Brief of Petitioner, LabMD, Inc., at 3–6, *LabMD*, 894 F.3d 1221 (No. 16-16270).

122 In fact, the court seemed to muddy the waters even further by stating in dicta that a grounding in established public policy was necessary for a finding of unfairness, essentially adding a fourth element to the previously established three-prong unfairness test. *See LabMD*, 894 F.3d at 1229 ("Thus, an 'unfair' act or practice is one which meets the consumer-injury factors listed above and is grounded in well-established legal policy."). The error of this construction is beyond the scope of this Note.

c. FTC v. D-Link Systems, Inc.*: A Court Treats Actual Harm as Necessary for Substantial Injury*

While the *LabMD* case was still pending in the Eleventh Circuit, a California district court stepped into that Section 5 jurisprudence void by dismissing an FTC data security case for failure to state a claim in *FTC v. D-Link Systems, Inc*.[123] In *D-Link*, the FTC alleged that a company sold wireless routers that had a widely known and easily exploitable security flaw that would allow "man-in-the-middle" attacks that could expose the entirety of a computer's files to a hacker.[124] The FTC argued that, as a result, sensitive consumer information was at "significant risk of being accessed by unauthorized agents,"[125] but it did not include any specific allegations of consumer harm stemming from the exposure.[126] D-Link moved to dismiss, and while the court found none of D-Link's arguments persuasive, it still opted to dismiss the case for failure to state a claim.[127] The court took issue particularly with the FTC's failure to allege any specific harm to consumers, stating that the FTC's allegations as pled "make out a mere possibility of injury at best,"[128] and distinguishing the case from *Wyndham* on the grounds that the FTC had shown specific harm in that case.[129] The court allowed the FTC leave to amend its complaint,[130] and the parties recently settled the case.[131]

Commentators quickly noted that the dismissal would make it difficult to pursue an unfairness claim based on exposure of consumer data without also showing evidence of actual misuse of that data.[132] The position of the court in *D-Link*, however, stands in conflict with the statement of the Third Circuit in *Wyndham*[133] that unreasonable data security practices may be unfair under Section 5 even before they result in any actual harms to consumers.[134] Viewing these cases alongside the Eleventh Circuit's continued silence in *LabMD*, it becomes clear that courts are struggling to

123 No. 3:17-cv-00039-JD, 2017 WL 4150873 (N.D. Cal., Sept. 19, 2017).

124 *See id.* at *1–2.

125 *See id.* at *1.

126 *See id.* at *5.

127 *See id.* at *5–6.

128 *Id.* at *5.

129 *See id.* at *5.

130 *See id.* at *6.

131 *See* Proposed Stipulated Order for Injunction and Judgment, *FTC v. D-Link Sys., Inc.*, No. 3:17-cv-00039-JD (N.D. Cal. filed July 2, 2019).

132 *See, e.g.*, Janis Kestenbaum, Rebecca Engrav & Erin Earl, *4 Takeaways From FTC v. D-Link Systems*, L. 360, (Oct. 6, 2017, 12:08 PM) https://www.law360.com/articles/971473/4-takeaways-from-ftc-v-d-link-systems [https://perma.cc/G7TN-FX2X].

133 799 F.3d 236 (3d Cir. 2015).

134 *See id.* at 246.

determine uniformly what the FTC needs to do in order to satisfy Section 5(n)'s substantial injury requirement in a data exposure case. At the core of the difficulty is the question of what Section 5(n) means when it requires that an unfair act "causes or is likely to cause substantial injury to consumers."[135] Answering that question requires interpreting the statute in light of its underlying purposes.

II. PURPOSES OF THE FTC ACT: PREVENTING MARKET FAILURES FROM HARMING CONSUMER WELFARE

Any serious attempt to parse the meaning of Section 5's unfairness provisions requires an understanding of the underlying purposes of the FTC Act and its consumer protection authority. From a policy perspective, consumer protection law is an essential and coequal partner of antitrust law, and both fit under a broader umbrella referred to as "consumer law." The object of consumer protection law, and of Section 5's consumer protection provisions, is the problem of "information asymmetries" that prevent consumer choices from creating efficient markets. Crucially, the purpose of the FTC Act is not to punish retroactively those who engage in market-distorting behavior, but to prospectively prevent such behaviors from harming consumer welfare.

C. Situating Section 5 in the Broader Context of Consumer Law

The FTC's consumer protection and antitrust missions, while based on slightly different statutory language and housed in separate bureaus,[136] are in essence two sides of the same policy coin[137]: as one former FTC Chairman put it, "[t]he policies that we traditionally identify separately as 'antitrust' and 'consumer protection' serve the common aim of improving consumer welfare and naturally complement each other."[138] In fact, some have argued that consumer protection and antitrust law should be grouped under one umbrella and collectively referred to as "consumer law."[139] This is an

---

135 15 U.S.C. § 45(n) (2018).

136 *See Bureaus and Offices*, FED. TRADE COMMISSION, https://www.ftc.gov/about-ftc/bureaus-offices [https://perma.cc/D5SR-FPWH].

137 *See* WILLIAM E. KOVACIC, THE FEDERAL TRADE COMMISSION AT 100: INTO OUR 2ND CENTURY 33 (2009), *available at* https://www.ftc.gov/sites/default/files/documents/public_statements/federal-trade-commission-100-our-second-century/ftc100rpt.pdf [https://perma.cc/B6RT-WM5Z].

138 Timothy J. Muris, The Interface of Competition and Consumer Protection, Prepared remarks at the Fordham Corporate Law Institute's Twenty-Ninth Annual Conference on International Antitrust Law and Policy 3 (Oct. 31, 2002) https://www.ftc.gov/sites/default/files/documents/public_statements/interface-competition-and-consumer-protection/021031fordham.pdf [https://perma.cc/4M7K-4MPN].

139 Joshua D. Wright, *The Antitrust/Consumer Protection Paradox: Two Policies at War*

especially worthwhile perspective for analyzing the underlying purposes of the FTC Act, given how the consumer protection mission grew out of the antitrust mission.[140] Thus, examination of the policies and assumptions undergirding antitrust law can prove valuable in illuminating the economic functions of the FTC's consumer protection authority, and this section will frequently make analogies to established facets of antitrust law.

At its core, consumer law seeks to ensure that markets, competition, and consumer choice function to deliver maximum consumer and social welfare.[141] The Supreme Court has famously and repeatedly referred to antitrust law as a "consumer welfare prescription."[142] Consumer welfare is also undoubtedly the goal of consumer protection law, but the mechanism for achieving that goal is equally important to note: consumer law in general seeks to maximize consumer welfare by "deliver[ing] well-functioning markets."[143] The policy decision at the heart of the initial enactment of antitrust laws in the United States was that competition and consumer choice would deliver the most desirable allocation of resources and the maximum social welfare[144]—this is why, in *National Society of Professional Engineers v. United States*,[145] the Supreme Court dismissed the contention that price competition among engineers could have a negative impact on the public interest as "nothing less than a frontal assault on the basic policy" of United States antitrust law.[146] While consumer protection law has not historically relied on economic arguments about the functioning of markets in the same way that antitrust law has,[147] the underlying aim of both the antitrust and consumer protection provisions of Section 5 is still very much "to protect consumers by ensuring that markets work well."[148]

---

with Each Other, 121 YALE L.J. 2216, 2218 (2012).

140 *See supra* Section I.A.

141 Neil W. Averitt & Robert H. Lande, *Consumer Sovereignty: A Unified Theory of Antitrust and Consumer Protection Law*, 65 ANTITRUST L.J. 713, 713–14 (1997).

142 Reiter v. Sonotone Corp., 442 U.S. 330, 343 (1979) (quoting ROBERT BORK, THE ANTITRUST PARADOX 66 (1978)); *see also* NCAA v. Bd. of Regents of Univ. of Okla., 468 U.S. 85, 107 (1984) (quoting *Reiter*, 442 U.S. at 343); Arizona v. Maricopa Cnty. Med. Soc'y, 457 U.S. 332, 367 (1982) (Powell, J., dissenting) (quoting *Reiter*, 442 U.S. at 343).

143 Mark Armstrong, *Interactions Between Competition and Consumer Policy*, COMPETITION POL'Y INT'L, 97, 98 (2008).

144 *See* ANDREW I. GAVIL ET AL., ANTITRUST LAW IN PERSPECTIVE, 34–35 (3d ed. 2017).

145 435 U.S. 679 (1978).

146 *Id.* at 695. The Court here was referring to the policy of the Sherman Antitrust Act, 15 U.S.C. §§ 1–7 (2018), but given that the FTC Act arose out of concern that the Supreme Court had gutted the Sherman Act, *see supra* Section I.A.1, the discussion of the underlying policy is just as relevant to the FTC Act.

147 Armstrong, *supra* note 143, at 99.

148 KOVACIC, *supra* note 137, at 33.

This object of consumer law, the well-functioning market, is reasonably straightforward in theory: a fundamental premise of classical economics is that when markets operate under optimal conditions, they allocate resources in a way that generates maximum social surplus, meaning that both producers and consumers gain the greatest possible net benefits from the allocation of goods.[149] Consumer preferences dictate demand for goods and services, and as producers match output to demand, the price for the good or service settles at a point of equilibrium. At this perfect equilibrium point, most consumers will receive more value out of the product or service than they pay for it, and consumer and producer welfare cannot be increased without decreasing the value of the other.[150] It is in this sense that a perfectly functioning market is supposed to maximize consumer welfare.

Of course, market conditions are frequently imperfect, and certain conditions can lead markets to fail in ways that prevent them from maximizing consumer welfare.[151] Such "market failures" occur "when functioning markets fail to realize full gains from trade through efficient production,"[152] and they can take several forms: monopoly conditions may allow a producer to raise prices at the expense of overall consumer welfare,[153] for example, or imperfect information may lead consumers to pay more for a good or service than it is actually worth to them.[154] The primary object of consumer law is preventing and ameliorating the conditions that lead to such market failures and reductions in consumer welfare, "with antitrust policy focusing on market failures associated with the creation of market power and consumer protection emphasizing instances in which, despite ample competition, consumer welfare is threatened by information asymmetries and deception."[155]

D. Information Asymmetries as the Object of Section 5's Consumer Protection Provisions

Market-distorting information asymmetries are the economic problem that Section 5's consumer protection provisions address. Economists use the term "information asymmetry" to describe a situation in which one party to a transaction—typically the seller—has more information about the product

149 *See* DAVID L. WEIMER & AIDAN R. VINING, POLICY ANALYSIS 62 (6th ed. 2017).

150 *See id.* at 60.

151 *Id.* at 74.

152 Wright, *supra* note 139, at 2222.

153 GAVIL ET AL., *supra* note 144, at 30–32.

154 WEIMER & VINING, *supra* note 149, at 104–05. Economists also traditionally recognize public goods and externalities as common market failures, *id.* at 71, but these are not as fully within the scope of consumer law.

155 Wright, *supra* note 139, at 2218.

or its attributes than the other.[156] If the consumer's lack of information leads to an overestimation of the value of the product—by concealing the health costs that will result from consumption of a drug, for example—the consumer will receive less value from the product than expected, resulting in a transfer of surplus from the consumer to the producer, as well as a net "deadweight" loss to society.[157] Paradigm examples of this type of market failure include consumption of products like "exploding toasters and toys tainted with dangerous levels of lead"[158]—if consumers were aware of the risk that the toaster would explode or that the toy was laden with lead, demand would shrink, and the few who did elect to purchase the products would do so at a much lower price. Because they do not have information about the risk of explosion or lead content, however, consumers will pay more for the product than it is worth to them, and consumer welfare will decrease.

Economically speaking, the FTC's consumer protection authority under Section 5 represents a policy intervention in market failures due to information asymmetries. This concept is borne out in a number of ways, not the least of which is in the FTC's consumer protection cases themselves: an information asymmetry can be found at the heart of nearly every Section 5 consumer protection action.[159] This is certainly true of the FTC's deception cases—after all, deception by nature is only successful insofar as it creates an asymmetry of information.[160] Looking back at *FTC v. Raladam*,[161] for example, the problem with making false claims about diet pills can be seen as a problem of information asymmetry in which consumers, believing the false claims, will pay more for the product than it is actually worth to them, resulting in a loss of consumer welfare and net loss to society. Crucially, this harm was not cognizable under the FTC Act in its initial iteration as an antitrust statute,[162] and this type of conduct became subject to the regulation

156 *See* WEIMER & VINING, supra note 149, at 104–05. Market distortions are less likely to occur when the buyer has more information than the seller, or when the buyer is underestimating the value of the product, as the seller has strong incentives to discover and provide positive information about the product. *See id.* at 105.

157 *See id.* at 104–05.

158 Wright, *supra* note 139, at 2222.

159 *Cf.* Neil W. Averitt, *The Meaning of "Unfair Acts and Practices" in Section 5 of the Federal Trade Commission Act*, 70 GEO. L.J. 225, 251–52 (1981) (detailing that "[a]n unfairness action . . . will be appropriate only when [the business's] methods have undermined the ability of consumers to protect themselves," a situation that does not occur when "a transaction is characterized by the absence of coercion [and] the possession of material information").

160 *See id.* at 265.

161 283 U.S. 643 (1931).

162 *See id.* at 654.

of the FTC Act only after the passage of the Wheeler-Lea Amendments.[163]

The concept of information asymmetry also explains the role of materiality[164] in deception cases: if the information the seller provides is not "likely to affect a consumer's choice of or conduct regarding a product,"[165] it can result in no distortion to the market.

More importantly for this analysis, it is also fair to characterize most of the FTC's unfairness cases as primarily revolving around information asymmetries.[166] In the FTC's model Section 5 unfairness case, *International Harvester*,[167] the central issue was that the manufacturer knew that the tractors it sold had a fuel-geysering problem, but failed to inform the consumers who used the product.[168] In other words, the market suffered from an information asymmetry problem—consumers paid for and expected a tractor with ordinary safety hazards, and instead received a tractor with extraordinary safety hazards. It is not difficult to imagine that, had consumers known about the dangers, they would have valued the product differently, and had the company placed warning labels on the tractors, consumers would have either paid a different price for them or utilized them in a way that accounted for the safety risks.[169] Either way, the ultimate effect of the company's failure to provide safety information was a dramatic and tragic loss in consumer welfare.

E. The Preventative Design of Section 5

"The purpose of the Federal Trade Commission Act is to protect the public, not punish the wrongdoer."[170] A definitive policy feature of the FTC

---

163 Wheeler-Lea Act of 1938, Pub. L. No. 75-447, 52 Stat. 111; *see also* Holloway v. Bristol-Myers Corp., 485 F.2d 986, 993–94 (D.C. Cir. 1973) (detailing how the Wheeler Lea Amendments "provide[d] the amendments to the Federal Trade Commission Act that the FTC had sought . . . [i]n its effort to overrule the *Raladam* case").

164 *See* DECEPTION STATEMENT, *supra* note 84 (stating that a representation must be material in order to constitute a deceptive act or practice under Section 5).

165 *Id.* The statement goes on to state that "[i]njury exists if consumers would have chosen differently but for the deception. . . . Thus, injury and materiality are different names for the same concept." *Id.*

166 It is worth noting here that the FTC has identified high pressure sales tactics as an unfair practice, *see* UNFAIRNESS STATEMENT, *supra* note 40, at 1074, but this type of conduct does not appear to involve information asymmetries. It does, however, result in market distortions and decreased consumer welfare, as coerced consumers end up purchasing goods regardless of their value. *See, e.g.*, *Holland Furnace Co. v. FTC*, 295 F.2d 302, 303–04 (7th Cir. 1961) (sellers offered free furnace inspections and then refused to reassemble consumers' home furnaces, compelling the customers to purchase goods or services).

167 104 F.T.C. 949 (1984).

168 *Id.*

169 *See id.* 950–51.

170 Orkin Exterminating Co. v. FTC, 849 F.2d 1354, 1368 (11th Cir. 1988) (quoting

Act is that it was designed to prevent unfair and deceptive practices before they harm consumers.[171] Consumer law, rooted as it is in economic predictions about specific market dynamics, is fundamentally predictive—on the antitrust side of consumer law, for example, certain conduct that is known to harm competition and consumer welfare gains condemnation regardless of a showing of actual harm,[172] and both the FTC and the Department of Justice have the ability to block mergers before they are completed based on their likely adverse impacts to competition.[173] Congress incorporated this prospective focus into the initial passage of the FTC Act,[174] and early court decisions recognized that Section 5 empowered the Commission to identify and "stop all those trade practices *that have a capacity or a tendency* to injure."[175]

This goal of prevention carried over explicitly into congressional debates about the addition of the consumer protection provisions of Section 5: "An additional factor ameliorating Congress's concern [about abusive enforcement] at the time of the 1938 expansion of the Act to include consumer protection was that the FTC's power was 'merely preventative and cooperative rather than penal.'"[176] Indeed, when it comes to the FTC's history of policing deceptive practices, the policy of prevention shines through: it is extremely telling, for example, that in order to succeed on a deception claim, the FTC does not need to demonstrate actual harm to consumers as a result of the deception.[177] In essence, courts and the FTC treat practices that meet the elements for deception under Section 5 in the same way that they treat per se violations of antitrust laws—preventing the practices because their negative impacts on consumer welfare are well-known and easily predictable.

Given that "deception is one specific but particularly important application" of unfairness under the FTC Act,[178] there is little reason to believe that Section 5's preventative purpose does not carry over to unfairness actions. Section 5 jurisprudence has in fact identified practices that seem to automatically qualify as unfair, such as mass unilateral

---

Regina Corp. v. FTC, 322 F.2d 765, 768 (3d Cir. 1963)).

171 HOOFNAGLE, *supra* note 20, at 37.

172 *See, e.g.*, NCAA v. Bd. of Regents of Univ. of Okla., 468 U.S. 85, 100 (1984).

173 *See* Hart-Scott-Rodino Antitrust Improvements Act of 1976, 15 U.S.C. § 18a (2018).

174 51 CONG. REC. 12,791 (1914) (statement of Sen. White) (stating that FTC Act provisions are "largely preventive in their purposes and objects").

175 Sears, Roebuck & Co. v. FTC, 258 F. 307, 311 (7th Cir. 1919) (emphasis added).

176 Victor E. Schwartz & Cary Silverman, *Common-Sense Construction of Consumer Protection Acts*, 54 U. KAN. L. REV. 1, 11 (2005) (quoting S. REP. NO. 74-1705, at l (1936)).

177 *See* DECEPTION STATEMENT, *supra* note 84 ("The issue is whether the act or practice is likely to mislead, rather than whether it causes actual deception.").

178 *In re* Int'l Harvester Co., 104 F.T.C. 949, 1064 (1984).

termination of consumer contracts[179] or unauthorized billing.[180] Granted, this notion appears to contradict the Commission's statement in *International Harvester* that "[u]nlike deception, which focuses on 'likely' injury, unfairness cases usually involve actual and completed harms."[181] On closer examination, however, this passage ultimately bolsters the idea that unfairness actions can be prospective in scope because it treats the word "likely" as the operative term differentiating the focus of deception and unfairness. As codified in Section 5(n), a finding of unfairness requires that the act or practice in question "causes *or is likely to cause* substantial injury to consumers."[182] If "likely" is indeed the operative difference between a focus on prospective or completed harms, then Section 5(n) enables the FTC to prospectively enjoin harmful practices under its unfairness power in the same way that it does with its deception power.

The remedies structure of the FTC Act is also fundamentally forward-looking: as the Supreme Court has stated, "[o]rders of the Federal Trade Commission are not intended to impose criminal punishment or exact compensatory damages for past acts, but to prevent illegal practices in the future."[183] It is crucial to note that the FTC Act enables the Commission primarily to seek injunctive relief against unfair and deceptive practices.[184] By filing a complaint in a federal district court, the FTC may have the opportunity to seek some amount of consumer redress for Section 5 violations, but only those that are within the equitable powers of the court to grant.[185] The only instance in which the FTC may seek civil penalties is for a violation of an existing order, or for a violation of an administrative rule.[186] Thus, for Section 5 violations, neither compensatory, consequential, nor punitive damages are ever on the table, as they would be in a retrospective tort, contract, or criminal action for a completed harm. Accordingly, the remedies structure of the FTC Act best situates the Commission to address likely consumer harm.

After synthesizing the underlying economic policy and prospective design, a clearer picture of the purposes of the FTC Act's consumer protection provisions emerges: the prevention and remediation of information asymmetries that distort markets and reduce consumer welfare.

---

179 *See* Orkin Exterminating Co. v. FTC, 849 F.2d 1354, 1368 (11th Cir. 1988).

180 *See* Muris, *supra* note 138, at 4, 5.

181 *Int'l Harvester*, 104 F.T.C. at 1061.

182 15 U.S.C. § 45(n) (2018) (emphasis added).

183 FTC v. Ruberoid Co., 343 U.S. 470, 473 (1952).

184 *See* 15 U.S.C. § 45(b).

185 *See id.* § 53(b).

186 *See id.* § 45(l)–(m).

It is in this context that the meaning of "substantial injury to consumers" should be considered.

III. UNDERSTANDING EXPOSURE OF CONSUMER DATA ITSELF AS "SUBSTANTIAL INJURY TO CONSUMERS"

As discussed above, an act or practice may only qualify as unfair under Section 5 if it "causes or is likely to cause substantial injury to consumers."[187] When courts ask, as the court did in *D-Link*,[188] whether the FTC has shown enough actual harm to consumers to satisfy the substantial injury requirement for an unfairness claim under Section 5, they are asking the wrong question (or only part of the right question). Recalling the underlying purposes of the FTC Act,[189] the real question that courts should be asking is whether the challenged practice typically causes significant reductions in consumer welfare via information asymmetries. Given the focus of the FTC Act on market distortions, the most sensical interpretation of the phrase "substantial injury to consumers" in Section 5(n) is that it has occurred when an information asymmetry has significantly undermined consumer choice and decreased consumer welfare. From there, it becomes possible to see that exposure of sensitive consumer information should be sufficient to constitute a substantial injury for the purposes of proving an unfair act or practice under the FTC Act, even absent a showing of tangible or financial harm stemming from the exposure. Data security is an arena rife with market-distorting information asymmetries, and given the frequency and sophistication of data theft, there is a high likelihood that serious consumer injury will result from any given data exposure.

A. Interpreting "Substantial Injury to Consumers" as Reductions in Consumer Welfare from Information Asymmetries

Given that reasonable disagreement exists as to the plain meaning of "substantial injury to consumers" in Section 5(n),[190] it is proper to turn to the underlying purposes of the statute in interpreting its meaning. As discussed above, in terms of policy, the consumer protection provisions of Section 5 should be understood in conjunction with the statute's antitrust provisions as part of the broad umbrella of consumer law, which aims to prevent consumer-welfare-reducing market failures.[191] A careful reading of the language of the Unfairness Statement on a granular, textual level underscores

187 *Id.* § 45(n).

188 *See* FTC v. D-Link Sys., Inc., No. 3:17-cv-00039-JD, 2017 WL 4150873, at *5 (N.D. Cal. Sept. 19, 2017).

189 *See supra* Part II.

190 *See supra* Section I.B.2.

191 *See supra* Section II.A.

this reading of Section 5's consumer protection provisions as focused on market dynamics: the statement uses plural constructions in describing what types of conduct or effects can constitute a finding of unfairness,[192] indicating a focus on broad, market-wide distortions. The broader context of the statement is also helpful here: the inclusion of the requirement that "the injury must not be outweighed by any offsetting consumer or competitive benefits"[193] is indicative of an attempt to direct the focus of the unfairness doctrine onto broad economic impacts. This is further borne out by the insistence that "[e]motional impact and other more subjective types of harm . . . will not ordinarily make a practice unfair,"[194] which clearly signals an intent to move the focus of the FTC Act away from subjective issues of morality and decency and situate it instead in the context of broad economic dynamics and predictable inefficiencies.

For the purposes of interpreting the codification of the Unfairness Statement in Section 5(n), the question then becomes what market distortions constitute "substantial injury to consumers."[195] For the answer, an analogy to antitrust law is again useful: just as the "antitrust injury" is understood as a reduction in consumer welfare due to a loss of competition,[196] the "consumer protection injury" should be understood as a reduction in consumer welfare due to "information asymmetries."[197] As noted above, this interpretation is borne out by the FTC's unfairness case law: a reduction in consumer welfare from an information asymmetry undergirds nearly every successful unfairness action.[198] It would be misguided to define the substantial injury requirement by anything other than the type of harm that Section 5's consumer protection provisions are intended to prevent: consumer-welfare-reducing information asymmetries.

Perhaps most importantly, this interpretation of Section 5(n) does not require a showing of actual, completed harm to consumers in order for the FTC to succeed on an unfairness claim.[199] This is not, however, as radical as

---

192 UNFAIRNESS STATEMENT, *supra* note 40, at 1073 ("In most cases a substantial injury involves monetary harm, as when sellers coerce consumers into purchasing unwanted goods or services or when consumers buy defective goods or services on credit but are unable to assert against the creditor claims or defenses arising from the transaction. Unwarranted health and safety risks may also support a finding of unfairness.").

193 *Id.*

194 *Id.*

195 15 U.S.C. § 45(n) (2018).

196 *See, e.g.*, Brunswick Corp. v. Pueblo Bowl-O-Mat, Inc., 429 U.S. 477, 487–89 (1977) (stating that antitrust laws "intended to forestall" injuries to competition).

197 *See* Wright, *supra* note 139, at 2218.

198 *See supra* Section II.B.

199 Still, a showing of actual, completed harm is certainly persuasive evidence of a reduction in consumer welfare due to information asymmetry.

it sounds—a key feature of the Section 5 jurisprudence on deception, which is subsumed by unfairness,[200] is that the FTC need only demonstrate a likelihood that consumers will be deceived by the conduct.[201] Consumer protection law, like its antitrust companion, is no stranger to predictive interventions to prevent likely harm to consumers.[202] Still, as the *D-Link* decision indicates, arguments exist for interpreting the substantial injury requirement as an injury-in-fact requirement.[203] Critics of the FTC's data protection authority have described unfairness claims without a showing of actual harm as "significantly out of step with current constitutional-standing jurisprudence," arguing that the substantial injury requirement should be interpreted as incorporating the requirements for Article III standing.[204]

While it is true that the word "injury" exists both in Section 5(n) and the requirements for Article III standing, this interpretation has two major flaws. First, it would create a surplusage in the statutory language given that the FTC already has the standing required for all cases and controversies.[205] Perhaps more importantly, though, such an interpretation would essentially turn Section 5 into a tort or contract system without tort or contract remedies[206]—if the FTC had to demonstrate injury in fact in order to satisfy the substantial injury requirement, it would be no more effective than a private plaintiff in the tort system at holding entities liable for irresponsible protection of consumer data. At the same time, the Commission would not be able to seek the kinds of damages that come with tort liability.[207] Put another way, while Article III standing doctrines regarding injury-in-fact are valuable for protecting defendants from frivolous suits that carry the threat of huge punitive damages, they are less appropriate in the context of FTC unfairness actions in which such remedies are unavailable.

Interpreting the substantial injury requirement of Section 5(n) to mean significant reductions in consumer welfare due to information asymmetries does not, however, mean that every information asymmetry in the marketplace merits a Section 5 intervention. Rather, "market failure is a necessary but not sufficient condition for regulation."[208] After all, Section 5(n) still requires the injury to be "substantial" in order to warrant a finding

---

200 *See In re* Int'l Harvester Co., 104 F.T.C. 949, 1064 (1984).

201 *See* DECEPTION STATEMENT, *supra* note 84.

202 Again, the language of Section 5(n) requires that conduct is unfair if it "causes *or is likely to cause* substantial injury to consumers." 15 U.S.C. § 45(n) (2018) (emphasis added).

203 *See, e.g.*, Lammie & Andrews, *supra* note 12, at 11.

204 *Id.*

205 U.S. CONST. art. III, § 2.

206 *See supra* notes 183–186 and accompanying text.

207 *See* HOOFNAGLE, *supra* note 20, at 344.

208 Wright, *supra* note 139, at 2222 n.18.

of unfairness.[209] Additionally, certain types of information asymmetries tend to be corrected by market forces—secondary markets compiling information about products and services may alleviate inefficiency due to information asymmetry, as will sampling of search goods and experience goods.[210] It is when these kinds of corrective mechanisms are unavailable, however, that information asymmetries can lead to the kind of significant reduction in consumer welfare that is cognizable as a substantial injury under the FTC Act.

B. Unreasonable Data Security Practices Create Information Asymmetries That Typically Lead to Significant Reductions in Consumer Welfare

Natural market-corrective mechanisms are notably absent in the consumer data security arena, where market-distorting asymmetries are plentiful and consumers are unable to maximize their welfare by "distinguish[ing] secure products from insecure ones."[211] The key problem, from an economic perspective, is that consumers have difficulty shopping for data security[212]—data security is too technically "complex and largely opaque"[213] to be a search good, meaning that consumers cannot evaluate the risks of data exposure before purchasing a product or service.[214] Instead, data security qualifies more as an experience good, meaning that consumers can evaluate its quality only after purchase.[215] While such a problem would ordinarily be solved by the emergence of secondary markets for valuable information[216]—restaurant reviews are a good example—data security also exhibits the special problem of post-experience qualities, meaning that

---

209 15 U.S.C. § 45(n) (2018).

210 WEIMER & VINING, supra note 149, at 106, 108–09.

> A good is a search good if consumers can determine its characteristics with certainty prior to purchase. For example, a chair in stock in a store is a search good because consumers can judge its quality through inspection prior to purchase. A good is an experience good if consumers can determine its characteristics only after purchase; examples include meals, hairstyling, concerts, legal services, and used automobiles.

Id. at 106.

211 *See* BRUCE SCHNEIER, CLICK HERE TO KILL EVERYBODY 133–34 (2018) (characterizing consumer data security as a "lemons market," in which "[b]asically, comparison shopping is impossible").

212 *See, e.g.*, HOOFNAGLE, *supra* note 20, at 341; James P. Nehf, *Shopping for Privacy Online: Consumer Decision-Making Strategies and the Emerging Market for Information Privacy*, 2005 U. ILL. J.L. TECH. & POL'Y 1, 29–32 (describing difficulties for consumers who attempt to factor privacy preferences into online activities).

213 SCHNEIER, *supra* note 211, at 134.

214 *See* WEIMER & VINING, supra note 149, at 106.

215 *See id.*

216 *See id.* at 109–10.

consumers cannot detect the full costs and effects of engaging with the product until long after purchase, and may not even be able to trace negative impacts back to their source.[217] In this instance—epitomized by the example of the long-term effects of a drug—economists would not expect primary or secondary markets to be particularly effective, and consumer-welfare-reducing inefficiencies are likely to persist.[218] Furthermore, as the Equifax breach dramatically demonstrated, consumer data security suffers from a third-party problem, in which consumers are not even aware of what entities are collecting their sensitive information. In this instance, consumer choice is entirely removed from the data security realm, preventing the emergence of any kind of functional market mechanism.

A glance at the FTC's record of data security cases once again reveals a focus on information asymmetries that impede consumer choice and reduce consumer welfare. For example, in the Commission's *Eli Lilly*[219] case, the underlying assumption was that if the consumers had known that the company would take such little care of their identities, they would have weighed that against the value of the service in deciding whether to sign up for a newsletter about Prozac.[220] Similarly, looking at the facts of *Wyndham*,[221] it is not difficult to imagine that if consumers had been aware that the company had failed to respond to multiple separate hacks,[222] the demand for Wyndham hotel bookings would have decreased, and consumers would have either opted not to provide their information to the company or would only have done so in exchange for a steep discount. The same characterization fits the *LabMD*[223] and *D-Link*[224] facts: lack of access to information about the companies' security practices prevented consumers from fully evaluating the costs and risks associated with providing their

217 *See id.* at 111.

218 *See id.*

219 *In re* Eli Lilly & Co., 133 F.T.C. 763 (2002).

220 *See id; see also* FED. TRADE COMM'N, No. 180821780-8780-01, COMMENT TO NATIONAL TELECOMMUNICATIONS AND INFORMATION ADMINISTRATION ON DEVELOPING THE ADMINISTRATION'S APPROACH TO CONSUMER PRIVACY 16 (2018), https://www.ftc.gov/system/files/documents/advocacy_documents/ftc-staff-comment-ntia-developing-administrations-approach-consumer-privacy/p195400_ftc_comment_to_ntia_112018.pdf [https://perma.cc/5K7V-RLAK] ("[C]hoice is important when the risk of harm might significantly increase, such as where the data is sensitive.").

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

222 *Id.* at 241–42.

223 *In re* LabMD, Inc., No. 9357 (F.T.C. July 29, 2016) (Public Opinion of the Commission).

224 FTC v. D-Link Sys., Inc., No. 3:17-cv-00039-JD, 2017 WL 4150873 (N.D. Cal., Sept. 19, 2017).

medical information to LabMD or purchasing routers from D-Link, likely leading to a loss in consumer welfare from the exposure of sensitive data.[225]

1. The Injuries That Consumers Bear from Data Exposure Are Substantial

Having established that exposure of consumer data creates market-distorting information asymmetries, it is crucial not to lose sight of the statutory language: specifically, Section 5(n) requires that the injury to consumers be "substantial."[226] After all, the FTC Act does not recognize "trivial or merely speculative harms."[227] To be clear, though, the losses in consumer welfare associated with data exposure are far from trivial: rather, exposure of consumer data can have disastrous impacts on consumers, and consumers incur real costs when attempting to avoid or mitigate the effects of data exposure.

First, the costs that can occur from exposure of sensitive consumer data are enormous and extremely consequential. Identity theft is one of the main harms that can result from exposure of consumer data: one study found that in 2016 alone, "6.15 percent of consumers became victims of identity fraud," resulting in losses of roughly $16 billion.[228] Another report found that for the 17,576,200 victims of identity theft in the United States in 2014, the average loss suffered as a result of the identity theft came to $1,343.[229] While not all identity theft stems from poor handling of consumer data, even if a quarter of the 2016 losses stemmed from poor data security practices, it would constitute an overall consumer welfare reduction of $4 billion. Identity theft can also have more than monetary costs: at the FTC's workshop on informational injury, one of the panelists illustrated the effects of medical identity theft by relaying the story of a mother who lost custody of her children as a result of an impostor using her identity to go to several hospitals in search of painkillers.[230] Less serious losses have satisfied the substantiality

---

225 *See D-Link*, 2017 WL 4150873, at *1; *LabMD*, No. 9357 at 5.

226 15 U.S.C. § 45(n) (2018).

227 UNFAIRNESS STATEMENT, *supra* note 40, at 1073.

228 *Identity Fraud Hits Record High with 15.4 Million U.S. Victims in 2016, Up 16 Percent According to New Javelin Strategy & Research Study*, JAVELIN STRATEGY (Feb. 1, 2017), https://www.javelinstrategy.com/press-release/identity-fraud-hits-record-high-154-million-us-victims-2016-16-percent-according-new [https://perma.cc/X23S-CKE3].

229 ERIKA HARRELL, BUREAU OF JUSTICE STATISTICS, U.S. DEP'T OF JUSTICE , VICTIMS OF IDENTITY THEFT, 2014 (2017), https://www.bjs.gov/content/pub/pdf/vit14.pdf [https://perma.cc/GD2L-BCLG].

230 Statement of Pamela Dixon, Founder and Executive Director of the World Privacy Forum, FTC Informational Injury Workshop, Segment 2, Panel 1 (Dec. 12, 2017), https://www.ftc.gov/system/files/documents/videos/informational-injury-panel-1-injuries-101/ftc_informational_injury_transcript_segment_2.pdf [https://perma.cc/KT74-RQC7].

requirement,[231] and it is hard to imagine that consumers consider the risk of such losses immaterial to their purchasing decisions.

When sensitive data is exposed, it typically falls on consumers to bear the costs of mitigating the risk of injury, which itself entails substantial costs. Many end up simply paying for fraudulent charges.[232] Those who do not tend to incur significant transaction costs from disputing such charges.[233] Checking credit reports, instituting credit freezes, getting new credit cards, and purchasing identity protection are all costs that reasonable consumers incur in response to exposure, even when there is no evidence that a thief or hacker has in fact acquired the information or attempted to steal an identity.[234] The FTC has considered the impact of similar kinds of costs in the context of "drip pricing"—the practice common in hotel and airfare booking of gradually adding fees onto the initial price quote—and has found that saddling consumers with such "cognitive costs" can undermine consumer choice and result in market inefficiencies.[235] Thus, even when consumers do not suffer direct economic loss from data exposure, they still incur costs that they could not have factored into their purchasing decisions, resulting in an overall reduction in consumer welfare.

2. Data Exposure Is Likely Enough to Result in Consumer Harm

Even with an understanding of the harms that often do result from exposure of consumer data, the question remains in unfairness cases of whether a particular exposure of sensitive data is "*likely* to cause substantial injury to consumers"[236] as required by Section 5(n). The amount of identity theft and fraud that results from data exposures, however, indicates that reductions in consumer welfare are sufficiently likely to occur, thereby satisfying the substantial injury requirement, especially given the preventative purpose of the FTC Act. According to one study, in the wake of 1,579 publicly disclosed data breaches in 2017[237]—more than half of which were the result of hacking[238]—more than 14 million credit and debit card

---

231 *See, e.g.*, Complaint at 7–9, *In re* Facebook, Inc., No. C-4365 (F.T.C. July 27, 2012) (alleging unfair practices where Facebook overrode users' chosen privacy settings without informing them).

232 HOOFNAGLE, supra note 20, at 224.

233 *Id.*

234 *Cf. id.* at 221–22.

235 MARY W. SULLIVAN, ECONOMIC ISSUES: ECONOMIC ANALYSIS OF HOTEL RESORT FEES 1, 4 (2017).

236 15 U.S.C. § 45(n) (2018) (emphasis added).

237 IDENTITY THEFT RES. CTR., 2017 ANNUAL DATA BREACH YEAR-END REVIEW 3 (2018).

238 *Id.* at 4.

records were exposed,[239] and more than 157 million Social Security numbers were exposed.[240] The likelihood of misappropriation of such data to the detriment of consumers is high, especially given the speed and sophistication with which cybercriminals operate—in one study conducted by the FTC, it took only nine minutes between when consumer data was exposed and when an identity thief attempted to make use of it.[241] Theft is fundamentally different in the cyber setting than it is in the physical world—it scales well, and it is systematized by thieves scanning for data exposures and security vulnerabilities.[242] Contrary to what Wyndham tried to argue, maintaining lax data security is not like installing a faulty lock on a hotel room door[243]—rather, it is more like leaving a faulty lock on a hotel room door while having full knowledge that every night an army of ninjas will attempt to infiltrate every guest's room. Put simply, if a vulnerability exists, hackers and thieves will almost certainly find and exploit it, making substantial injury to consumers likely.

IV. PROPOSAL: A BURDEN-SHIFTING APPROACH TO THE SUBSTANTIAL INJURY REQUIREMENT

Just because exposure of consumer data *can* constitute an unfair act or practice does not mean that it always will.[244] Recognizing that the purposes and design of the FTC Act permit a finding that exposure of information can constitute substantial injury absent a showing of actual harm, the issue remains of how the Commission and the courts should determine whether such an exposure satisfies the requirements of Section 5(n). Taking a cue from their approach to determining antitrust violations,[245] courts should apply a burden-shifting proof structure when determining whether "substantial injury" has occurred in a data breach unfairness action.[246] First,

---

239 *Id.* at 11.

240 *Id.* at 12.

241 *See* Statement of Tina Yeung, FTC Identity Theft: Planning for the Future Conference, Segment 1 (May 25, 2017), https://www.ftc.gov/system/files/documents/videos/identity-theft-planning-future-part 1/ftc_identity_theft_planning_for_the_future_transcript_segment_1.pdf [https://perma.cc/QJ6E-GBT5].

242 *See* HOOFNAGLE, *supra* note 20, at 223.

243 *See* FTC v. Wyndham Worldwide Corp., 799 F.3d 236, 246 (3rd Cir. 2015).

244 FEDERAL TRADE COMMISSION, *supra* note 93 ("[T]he mere fact that a breach occurred does not mean that a company has violated the law.").

245 *See, e.g.*, United States v. Microsoft Corp., 253 F.3d 34, 58–59 (D.C. Cir. 2001) (describing burden-shifting proof structure used to prove the "anticompetitive effect" of monopolist's conduct); United States v. Baker Hughes Inc., 908 F.2d 981, 982–83 (D.C. Cir. 1990) (describing burden-shifting proof structure used to establish that horizontal merger will lessen competition).

246 This section assumes that, if the FTC does show actual, completed harm stemming from the breach, then the substantial injury requirement would be satisfied and no further

if the FTC shows that a defendant's unreasonable data security practices led to an exposure of consumer data, it should establish a presumption that substantial injury to consumers has occurred. That presumption should be rebuttable, however, by a showing that either the type of data exposed was harmless, or that the degree of exposure was *de minimis*. Allowing rebuttal based on these two factors would allow for the possibility that some breaches do not create substantial consumer injury in the form of market distortions, keeping the FTC's unfairness authority tethered to the FTC Act's underlying goal of ensuring that markets and consumer choice deliver maximum consumer welfare. Throughout the analysis, the key question that courts would be seeking to answer is this: was the challenged conduct of the type that typically leads to significant market distortions and losses in consumer welfare?

A. The Initial Presumption of Substantial Injury

In order to trigger the burden-shifting analysis, the FTC would first be required to show that the defendant engaged in unreasonably lax data security practices. This would not be abnormal for an FTC data security case, given that the FTC typically treats unreasonableness of data security practices as a prerequisite for bringing a Section 5 data security action.[247] The departure from current practice, however, would be that a showing of unreasonableness would establish a rebuttable presumption that the "substantial injury" requirement has been met. Given the scale, speed, and sophistication of hacking and identity theft operations,[248] it makes sense to apply such a presumption. Application of a presumption of injury based on certain conduct also meshes well with the prospective nature of the FTC Act—prediction and presumption of harm is indeed a central feature of consumer law generally, and presumptions of economic injury have long played a role on the antitrust side of consumer law.[249] Finally, if the defendant is unable to produce any evidence to rebut the presumption, courts would be able to end the "substantial injury" analysis quickly.

B. Rebuttal of the Presumption Based on Type of Data Exposed or Scope of Breach

Once the FTC has demonstrated unreasonable data security practices and triggered the presumption of substantial injury to consumers, the burden of production would shift to the defendant, who would have a chance to rebut

---

analysis would be necessary.

247 *See* FEDERAL TRADE COMMISSION, *supra* note 93.

248 *See supra* Section III.B.2.

249 *See supra* Section II.C.

the presumption. The defendant would be able to rebut the presumption by producing evidence either that the data exposed was not the type that tends to injure consumers when exposed, or that the exposure was so minor in scope that its occurrence would not have a tendency to lead to consumer harm.

1. Rebutting the Presumption Based on Type of Data Exposed

One option available to defendants for rebutting the presumption of substantial injury would be to produce evidence that the type of data exposed was not of the type that, when exposed, frequently leads to consumer harms. There are, after all, plenty of types of data that do not create a high likelihood of consumer injury when exposed: strongly encrypted data, for example, is typically indecipherable when misappropriated, and thus its exposure is unlikely to result in consumer injury.[250] Similarly, with data about consumers that is already publicly available—anything that a consumer typically puts on a public social media platform, for example—it is hard to see how its re-exposure in a data breach would lead to significant market distortions. A list of harmless data types could go on and on,[251] but the point is that if the defendant can show that the type of data exposed is not one that typically leads to consumer harm, it would rebut the presumption of substantial injury, shifting the burden of proof back to the FTC to demonstrate either that consumers actually were injured by the exposure, or as a matter of fact at trial that the type of data exposed does tend to lead to injury.[252]

There are, of course, plenty of data types that courts would immediately recognize as likely to cause injury when exposed, and which would block a rebuttal based on data type: Social Security numbers and credit card information, for example, are the kinds of data that consumers ordinarily take steps to protect. To borrow from the FTC's deception lexicon, these types of data are likely material to consumers—that is, an entity's ability to keep this kind of data secure likely affects the consumer's purchase or engagement

---

250 *See* Thomas B. Pahl, *Stick with Security: Store Sensitive Personal Information Securely and Protect It During Transmission*, FED. TRADE COMMISSION (Aug. 18, 2017, 8:59 AM), https://www.ftc.gov/news-events/blogs/business-blog/2017/08/stick-security-store-sensitive-personal-information-securely [https://perma.cc/FKV9-JWDE] ("Encryption is the process of transforming information so that only the person (or computer) with the key can read it. Companies can use encryption technology for sensitive data at rest and in transit to help protect it across websites, on devices, or in the cloud.").

251 *See, e.g.*, Spokeo, Inc. v. Robins, 136 S. Ct. 1540, 1550 (2016) (describing publication of an incorrect zip code as an example of harmless data error).

252 Some types of independently harmless information, when combined, can lead to harm: in *In re Eli Lilly & Co.*, 133 F.T.C. 763, 767–68 (2002), for example, the problem was not that the consumers' email addresses were exposed, but rather that their exposure revealed that they were interested in antidepression drugs, such as Prozac.

decision, and an entity's failure to reasonably protect this type of data appears to create a market distortion based on an information asymmetry. For guidance in determining what kinds of data would block the data-type rebuttal, courts should consider looking to state data breach notification statutes—in Virginia, for example, entities are obligated to inform consumers when names are exposed in combination with unredacted Social Security numbers, credit or debit card numbers, bank account numbers, driver's license numbers, or state identification numbers.[253] Medical records and tax information should also qualify as sufficiently likely to lead to injury, given that consumers ordinarily take steps to protect this information, and both types of information are valuable to identity thieves.

2. Rebutting the Presumption Based on Scope of Exposure

If the defendant is unable to rebut the presumption of substantial injury based on data type, the defendant could still rebut the presumption by producing evidence that the degree of exposure would not result in a likelihood of consumer harm—in other words, the defendant would have the opportunity to show that the exposure was *de minimis* in scope. The defendant could do so by producing evidence regarding either the degree of accessibility of the data, the length of the data exposure, or some combination of both. If, however, the FTC can show that a hacker or data thief did, in fact, exfiltrate the data from the entity whose data security conduct is in question, the rebuttal would not be available, as the data would have been exposed just about as fully as possible.

In the absence of evidence that hackers have exfiltrated the exposed data, one avenue by which the defendant could demonstrate a *de minimis* degree of exposure would be by producing evidence that the exposed data was minimally accessible despite any allegedly unreasonable data security practices. If sensitive data were inadvertently placed in a non-password-protected folder on an otherwise secured company server, for example, a court would have room to find that the exposure was *de minimis*, depending on how many and what type of employees could or did regularly access that folder. If data were stored on an internet-connected server that had no firewall protections and was using default access passwords as in *Wyndham*,[254] however, the rebuttal would not be available because the data was accessible in a way that increased the likelihood that it would be misappropriated. In either case, the Commission and courts would have to determine, in common law fashion, what degrees of accessibility do or do

253 VA. CODE ANN. § 18.2-186.6 (2018).

254 799 F.3d 236, 240–41 (3d Cir. 2015).

not increase the likelihood that data will be misappropriated in ways that lead to common harms like identity theft.

The second variable in the scope of exposure rebuttal would be the duration of data exposure—obviously, the greater the amount of time that data sits exposed, the greater the chances are that it will end up misappropriated in a way that will lead to consumer harm. Absent a showing that data was actually misappropriated, for example, a defendant could argue that leaving a server unprotected by a firewall for ten minutes would be unlikely to lead to harms like identity theft, regardless of what level of incompetence led to those ten minutes of exposure. Leaving the same server unsecured for several days, however, would be more likely to result in misappropriation, and thus would not qualify as *de minimis*. Crucially, whether the length of exposure is sufficiently short to rebut the presumption of substantial injury would also depend on the relative accessibility of the data during the exposure—recalling the FTC's study in which an identity thief attempted to use consumer data only nine minutes after it was exposed on a public website,[255] it would be safe to assume that a defendant who left sensitive consumer data on a public website for more than a few minutes would likely be unable to rebut the presumption of substantial injury.

C. Shifting the Burden of Proof Back to the FTC After Rebuttal

If the defendant is able to rebut the presumption of substantial injury, the ultimate burden of proof would remain with the FTC to satisfy the substantial injury element of an unfairness claim. Specifically, the FTC would have to prove that, despite the defendant's rebuttal, the type of data exposed or the scope of its exposure does, in fact, tend to lead to reductions in consumer choice and consumer welfare. While this would likely lead to reliance on expert testimony at trial, the advantage of the burden-shifting proof structure is that it would narrow the issues at trial: at least in proving substantial injury, the FTC would have to focus on the rebuttals presented by the defendant. Additionally, the number of cases that make it past the rebuttal stage would dwindle over time as courts would continually determine, as a matter of law, what fact patterns either allow for rebuttal or deny it.

D. The Proposed Standard Would Be Fair to Defendants in FTC Data Security Cases

While plenty of defendants in FTC data security cases would likely object to the possibility that the FTC could succeed on an unfairness claim without showing specific harm to consumers, the standard proposed above actually provides defendants with ample opportunity to contest FTC actions.

---

255 *See* Statement of Tina Yeung, *supra* note 241.

Most obviously, it allows defendants the opportunity to dispute each factor in the analysis, and to defeat an FTC claim by showing, for example, that the data exposure was *de minimis*. It also allows defendants to dispute the facts of the underlying conduct, or to argue to a court that the data security procedures utilized were, in fact, reasonable. Finally, the other two elements required for a finding of unfairness would still remain fair game: defendants may argue that consumers were reasonably able to avoid any injuries, or that the costs of increased data security to the data-holding entity outweighed the benefits to consumers. This last element ensures that the broad scope of the substantial injury requirement will not lead to excessive costs or inefficiencies that would deny consumers the benefits of competition.

CONCLUSION

Having established a standard for evaluating substantial injury in FTC data security unfairness claims, it is worthwhile to conclude by applying this standard to the facts of *LabMD*[256] and *D-Link*.[257]

Looking first at *LabMD*, the data at issue would certainly foreclose rebuttal based on data type: the records exposed included names, Social Security numbers and sensitive medical information,[258] all of which has a tendency to harm consumers when exposed.[259] Turning to the question of degree of exposure, the data were exposed for several months,[260] but the question of accessibility would provide the defendants with some room to argue for rebuttal: the data was available on a publicly discoverable folder on the LimeWire peer-to-peer network,[261] but it was not obvious that the folder contained sensitive consumer information.[262] The Commission grappled with this issue itself,[263] but the discovery of other LabMD materials from LimeWire in an identity theft ring bust would make clear that the data was accessible in a way that could lead to the harm of identity theft, thus defeating any rebuttal the defendant may have attempted. At that point, then, the substantial injury element would be satisfied, and the Commission or a court would move on in its analysis to the other elements of an unfairness claim.

Application of the proposed structure to the facts of *D-Link* would lead to a much different outcome than in the actual case. The court in *D-Link*

256 No. 9357 (F.T.C. July 29, 2016) (Public Opinion of the Commission).

257 No. 3:17-cv-00039-JD, 2017 WL 4150873 (N.D. Cal., Sept. 19, 2017).

258 *LabMD*, No. 9357, at 2.

259 *See supra* Section III.B.1.

260 *See LabMD*, No. 9357, at 1.

261 *See id.* at 3.

262 *See id.* at 21–22.

263 *See id.* at 21–23.

ended the case on a motion to dismiss,[264] but the proposed proof structure would allow an FTC unfairness claim to survive a motion to dismiss by sufficiently pleading that the defendant used unreasonable data security practices. At summary judgment, then, the presumption of substantial injury would apply, and the defendant would have the opportunity to rebut the presumption. The data exposed was certainly sensitive—tax files on computers connected to the routers in question were potentially accessible due to the vulnerability,[265] and it is safe to assume that most consumers also keep passwords and other sensitive information on their computers—so the data-type rebuttal would likely fail. Turning to a scope-of-exposure rebuttal, the length of time that the security vulnerability existed on the routers was roughly six years,[266] so the degree of accessibility would be key: if the defendant could produce evidence that the mechanism for exploiting the vulnerability was not easy or widely known in the hacking community, as the FTC alleged,[267] it would likely rebut the presumption of substantial injury. If not, however, the presumption of substantial injury would remain unrebutted.

Ultimately, in an economy increasingly driven by electronic commerce and in which consumers have less and less control over how data about them is collected, consumers need to be as confident that companies will protect their data as they are that their toasters will not explode, or that their vehicles will not spew hot fuel at them. With the help of the proof structure proposed above, the FTC and Section 5 will be able to work toward that end.

---

264 *See* FTC v. D-Link Sys., Inc., No. 3:17-cv-00039-JD, 2017 WL 4150873, at *1, *6 (N.D. Cal., Sept. 19, 2017).

265 *See id.* at *5.

266 *See id.*

267 *See id.* at *1, *5.