Journal of Business & Technology Law

Volume 12 | Issue 2 Article 5

The FTC, the Unfairness Doctrine, and Privacy by Design: New Legal Frontiers in Cybersecurity

Stuart L. Pardau

Blake Edwards

Stuart L. Pardau* and Blake Edwards**

The FTC, the Unfairness Doctrine, and Privacy by Design: New Legal Frontiers in Cybersecurity

I. INTRODUCTION

In June 2012, the Federal Trade Commission ("FTC" or the "Commission") filed a lawsuit against hotel company Wyndham Worldwide Corporation ("Wyndham"), alleging sub-par cybersecurity standards and violations of the FTC Act (the "Act" or "FTCA")),[1] highlighted by three data security breaches in 2008 and 2009.[2] A little

* Stuart L. Pardau (J.D. Stanford Law School) is an Associate Professor at the David Nazarian College of Business and Economics, California State University, Northridge, Department of Business Law.

** Blake Edwards (J.D. Pepperdine Law) writes about the legal industry for Bloomberg and is also in private practice.

more than a year later, in August 2013, the Commission brought an administrative action against LabMD, Inc., a small, little-known medical testing company in Atlanta, Georgia, alleging violations of the Act in connection with alleged security breaches in 2008 and 2012.[3]

Although the FTC complaints in the two actions appeared similar, following a format used consistently by the FTC in data breach actions,[4] the two cases were remarkably different. Perhaps most importantly, Wyndham is a Fortune 500 company which brought in upwards of $5 billion in revenue in 2015, and owns more than 55 hospitality brands, whereas LabMD had approximately 20 employees at the time it was sued.[5] The breaches which inspired the FTC to sue, as well as the alleged security failures, were quite different in the two cases as well. The case against Wyndham centered on three different breaches over a period of two years, compromising "more than 619,000 payment card account numbers," which were posted to a domain registered in Russia.[6] The breaches, according to the FTC, cost consumers "more than $10.6 million in fraud loss."[7] Wyndham's alleged failings were specific and egregious: according to the FTC, the company failed to use adequate firewalls, allowed payment card information to be stored in readable text, did not employ common user ID and password procedures, and two separate times failed to correct errors after major breaches.[8] By contrast, although the FTC alleged broad failures by LabMD to implement and maintain a comprehensive security program, the company's purported wrongdoing centered on the decision of a single employee to install P2P file sharing software on a company computer.[9] A file containing the personal information of LabMD customers was leaked through the

1. 15 U.S.C. §§ 41–58 (2012).

2. *See generally* Complaint for Injunctive and Other Equitable Relief, F.T.C. v. Wyndham Worldwide Corp., No. 2:12-cv-01365-SPL (D.N.J. June 26, 2012) [hereinafter *Wyndham Complaint*].

3. *See generally* Complaint, *In re* LabMD, Inc., (F.T.C. Aug. 29, 2013) (No. 9357), 2013 WL 4761163 [hereinafter *LabMD Complaint*].

4. *Compare LabMD Complaint*, *supra* note 3, at 3–5, *with Wyndham Complaint*, *supra* note 2, at 10–18.

5. *See Our Company*, WYNDHAM WORLDWIDE, http://www.wyndhamworldwide.com/category/our-company. The company's brands include Wyndham Hotels and Resorts, Ramada, Days Inn, and Super 8. *Wyndham Hotel Group*, WYNDHAM WORLDWIDE, http://www.wyndhamworldwide.com/category/wyndham-hotel-group. Wyndham Hotel Group, one of three subsidiaries of Wyndham Worldwide, also named in the complaint, has over 7,800 properties and 678,000 rooms in 72 countries. *Id*. For a discussion of the size of LabMD, see generally Cheryl Conner, *When the Government Closes Your Business*, FORBES (Feb. 1, 2014, 5:55 PM), http://www.forbes.com/sites/cherylsnappconner/2014/02/01/when-the-government-closes-your-business/#5b8 94fc53652.

6. F.T.C. v. Wyndham Worldwide Corp., 10 F. Supp. 3d 602, 609 (D.N.J. 2014) (citing to allegations contained in the F.T.C. Complaint).

7. *Id.*

8. *See infra* Section III.B.

9. *See infra* Section III.A.

file-sharing network, but to this day LabMD and the FTC are still fighting about whether consumers suffered any actual harm.[10]

The Commission's legal arguments against the two companies were, in the end, the same: their failure to employ "reasonable and appropriate measures" to protect consumers' information constituted an "unfair" act or practice under Section 5 of the FTC Act.[11] Twenty years ago, the Commission would not likely have made this "unfairness" argument in the cybersecurity context.[12] The underlying legal provision, Section 5, prohibits "unfair" and "deceptive" acts or practices, and when the FTC first began bringing Section 5 cases in the cybersecurity context, the Commission utilized the "deceptiveness" prong, going after companies that had promised consumers a certain level of security (in their privacy policies, for example), and then failed to deliver.[13] This tactic made sense for a time. The private sector was still wrestling with how to secure information in a new and quickly evolving connected world.

But in the absence of comprehensive cybersecurity legislation, which the FTC has been requesting from Congress since at least 2000, the Commission increasingly felt that prevailing security practices were putting consumers at risk, and the "deceptiveness" prong of Section 5 was insufficient to police cyberspace appropriately.[14] The Commission's decision to broaden its cybersecurity policing tactics to include the "unfairness" prong, and to pursue companies that had hewed to their privacy policies but nevertheless failed, in the eyes of the FTC, to implement adequately robust cybersecurity measures, has been controversial.

The cases against Wyndham and LabMD have been flashpoints in this discussion. In August 2015, after the district court's denial of Wyndham's motion to dismiss, the U.S. Third Circuit Court of Appeals issued the first major ruling on the FTC's application of the unfairness prong to cybersecurity: in general it was an endorsement of the FTC's approach and a victory for the Commission.[15] Wyndham

10. *See infra* Section III.E.

11. *LabMD Complaint* at 5; *see also Wyndham Complaint* at 2.

12. J. Howard Beales, FED. TRADE COMM'N, THE FTC'S USE OF UNFAIRNESS AUTHORITY: ITS RISE, FALL, AND RESURRECTION (May 30, 2003), http://www.ftc.gov/public-statements/2003/05/ftcs-use-unfairness-authority-its-rise-fall-and-resurrection [hereinafter Beales] ("[I]n the 1990's, the Commission almost entirely avoided the use of unfairness. It became the theory of last resort.").

13. *See infra* Section II.C.

14. *See* FED. TRADE COMM'N, PRIVACY ONLINE: FAIR INFORMATION PRACTICES IN THE ELECTRONIC MARKETPLACE: A REPORT TO CONGRESS 36 (2000) https://www.ftc.gov/sites/default/files/documents/reports/privacy-online-fair-information-practices-electronic-marketplace-federal-trade-commission-report/privacy2000.pdf [hereinafter 2000 Report, FED. TRADE COMM'N] ("[T]he Commission recommends that Congress enact legislation" that in conjunction with continuing self-regulatory programs, will "ensure adequate protection of consumer privacy online.").

15. *See infra* Section III.C.

subsequently settled.[16] As for LabMD, the legal battle goes on.[17] After almost three years of wrangling with the FTC, an administrative law judge granted LabMD dismissal in November 2015, but the Commission later overturned the judge's decision, concluding the administrative action, leaving LabMD with one final shot in a federal appeals court.[18] If the U.S. Eleventh Circuit Court of Appeals, the court that would likely hear LabMD's appeal, takes up the case on the merits, it would be the second major decision on the FTC's unfairness approach, possibly either setting a trend, if the Eleventh Circuit issues a ruling similar to the Third Circuit's in *Wyndham*, or creating a circuit split if the courts differ.

However *LabMD* turns out, the two cases provide fertile ground for discussing the government's evolving role in policing cybersecurity, and highlights the necessity for businesses that handle or store consumers' personal information to pay very close attention to what the FTC says about privacy and cybersecurity. So what exactly does the FTC expect? This article's contention is that the answer to that question, in a phrase, is "privacy by design." Although it was first introduced by the Commission in a 2010 privacy report, privacy by design, or PbD, was created by the former privacy commissioner of the province of Ontario in Canada, and dates back to the mid-1990s.[19] Generally speaking, PbD is an admonition that entities think about privacy holistically; to imbed it not only in the processes and procedures of the enterprise, but to broadly socialize the concept so that it becomes part of the organizational DNA. Historically, privacy had been considered as presenting some intellectually interesting issues, but organizationally was much less of a priority: a "nice to have," but not a "need to have." Indeed, the very concept of a "Chief Privacy Officer" ("CPO") only started becoming more commonly accepted within the past ten to fifteen years,[20] and even to this day, despite the need, frequently remains less visible and more marginalized within the organization or may not even exist at all.[21]

16. Press Release, Fed. Trade Comm'n, Wyndham Settles FTC Charges It Unfairly Placed Consumers' Payment Card Information at Risk (Dec. 9, 2015), https://www.ftc.gov/news-events/press-releases/2015/12/wyndham-settles-ftc-charges-it-unfairly-placed-consumers-payment.

17. *See infra* Section III.E.

18. *See infra* Section III.E.

19. *See infra* Section IV.A.

20. In the United States, the CPO position was reportedly first established in 1999 when internet advertising firm AllAdvantage appointed privacy lawyer Ray Everett-Church to the newly created role. Justine Brown, Rise of the Chief Privacy Officer, GOVERNMENT TECHNOLOGY (May 30, 2014), http://www.govtech.com/state/Rise-of-the-Chief-Privacy-Officer.html. The move sparked a trend that quickly spread among major corporations. *Id.* But the CPO position was truly solidified within the U.S. corporate world in November 2000 when Harriet Pearson was given the role with IBM. *Id.*

21. Sarah K. White, *5 Reasons You Need to Hire a Chief Privacy Officer*, CIO (Feb. 1, 2016 4:22 AM), http://www.cio.com/article/3027929/leadership-management/5-reasons-you-need-to-hire-a-chief-privacy-officer.html.

In sum, the operating principle of PbD is that privacy should be proactive, not reactive, and "baked in" to a product's or a service's design.[22] The concept has proven to be both popular and malleable. The FTC's version identifies four PbD principles: data security, reasonable collection limits, sound retention practices, and data accuracy.[23] These principles alone, outlined in the Commission's various reports on cybersecurity, are arguably too broad to be of significant value to businesses, but the Commission has pointed to its settlements with Facebook and Google in particular as useful guides for implementing PbD, and practical manifestations of the Commission's PbD principles also emerge in its other complaints and consent decrees.[24]

With fresh sanction from the Third Circuit to prosecute cases using the "unfairness" prong of Section 5, the Commission has considerable power to impose its PbD program.[25] The purpose of this paper is to explore the interplay between the Commission's unfairness doctrine, the Wyndham and LabMD cases, and privacy by design. Knowledge of these concepts and cases are critical to understanding the current state of cybersecurity regulation in the United States, and necessary for any business wanting to steer clear of the FTC's scrutiny. Part II briefly discusses the history of the FTC, the FTC Act, and the Commission's evolving unfairness doctrine as applied to cybersecurity. Part III discusses the Wyndham and LabMD cases in detail, including the Third Circuit's decision validating the Commission's use of the unfairness doctrine, and the FTC's recent dismissal of LabMD's appeal of an administrative law judge in its favor. Part IV introduces the concept of privacy by design, traces the history of the FTC's use of the concept, and makes some practical recommendations for companies wanting to stay out of the FTC's crosshairs. Part V sets forth a brief conclusion.

II. THE FTC AND DATA SECURITY

A. From Trust Busters to the Golden Rule

When President Woodrow Wilson signed the FTC Act into law in 1914, the Commission opened its doors the following year with a bold but nebulous mission: to "protect consumers and promote competition."[26] Enacted concurrently with the

22. *See infra* Section IV.A.

23. *See infra* Section IV.B.

24. For a full discussion of Facebook and Google settlements, see *infra* Section IV.B.

25. *See* F.T.C. v. Wyndham Worldwide Corp., 10 F. Supp. 3d 602, 610 (D.N.J. 2014) (finding that despite Wyndham's assertions, the FTC may nevertheless bring a claim under the unfairness prong of Section 5 of the FTC Act).

26. *Our History*, FED. TRADE COMM'N, http://www.ftc.gov/about-ftc/our-history (last visited Feb. 15, 2017) [hereinafter *Our History*, FED. TRADE COMM'N]. The Commission is composed of five Commissioners nominated by the President and confirmed by the Senate, each of whom serves a seven-year term and no more

Clayton Act,[27] the nation's first anti-trust law, the Act was originally designed, through its prohibition of "unfair methods of competition," to facilitate "trust busting" efforts against the industrial monopolies of the early 20th Century.[28] Senator Francis Newlands, one of the Act's principle architects, promised that the Commission "would 'destroy' monopoly, 'check monopoly in the embryo,' and secure 'pygmies' against 'giants.'"[29]

But as the economy grew in size and complexity, the FTC's authority widened, filling out a more expansive interpretation of its mission and morphing into a direct consumer protection agency overseeing a variety of economic sectors.[30] The most rapid expansion of the FTC's clout came in 1938, when, in response to court decisions limiting the Act's prohibition of "unfair methods of competition" to practices actually harming competitors and not consumers, Congress passed the Wheeler-Lea Amendment and expanded "Section 5" of the FTCA to encompass "unfair or deceptive acts or practices" as well as "unfair methods of competition"—"thereby charging the FTC with protecting consumers directly, as well as through its antitrust efforts."[31]

The expansion of the FTC's role was considerable. To illustrate, contrast the remarks of Senator Newlands, focused on leveling the playing field for competitors, with those of President Franklin Roosevelt, delivered 23 years later at the dedication of the FTC's current home at 600 Pennsylvania Ave., N.W.:

> *May this permanent home of the Federal Trade Commission stand for all time as a symbol of the purpose of the government to insist on a greater*

than three of whom may be from the same political party. *See Commissioners*, FED. TRADE COMM'N, http://www.ftc.gov/about-ftc/commissioners (last visited Feb. 15, 2017).

27. 15 U.S.C. §§ 12–27 (2012).

28. *Id.* § 41. "[T]he Clayton Act . . . links the FTC's original focus to ensuring a level playing field for businesses rather than the consumer protection focus we see today . . . . If one were to view what the FTC was in 1914, it would have primarily consisted of what is now known as the Bureau of Competition. This stands in stark contrast to the FTC of today, which on its website brands itself as the 'nation's consumer protection agency.'" Andrew Serwin, *The Federal Trade Commission and Privacy: Defining Enforcement and Encouraging the Adoption of Best Practices*, 48 SAN DIEGO L. REV. 809, 814 (2011).

29. Marc Winerman, *The Origins of the FTC: Concentration, Cooperation, Control, and Competition*, 71 ANTITRUST L.J. 1, 77 (2003) (quoting 51 Cong. Rec. 12,030, 12,867, 12,939 (1914)).

30. *See, e.g.*, Press Release, Federal Trade Comm'n, FTC Announces Results of Compliance Testing of Over 300 Funeral Homes (Feb. 25, 1998), http://www.ftc.gov/news-events/press-releases/1998/02/ftc-announces-results-compliance-testing-over-300-funeral-homes (discussing how the FTC has gone so far as to regulate funeral home compliance within the FTC regulations).

31. *Beales*, *supra* note 12 (quoting Act of Mar. 21, 1938, Pub. L. No. 75-447, 52 Stat. 111, 111); *see also* Winerman, *supra* note 29, at 96; F.T.C. v. Wyndham Worldwide Corp. (*Wyndham II*), 799 F.3d 236, 243 (3d Cir. 2015).

> *application of the golden rule to conduct the corporation and business enterprises in their relationship to the body politic.*[32]

In accordance with this new mission, the Commission's authority broadened.[33] It now used Section 5 and other statutes to oversee a number of areas of the economy in the name of consumer protection.[34] Today, the FTC polices everything from funeral homes,[35] vending machine companies,[36] telemarketing[37] and mail marketing schemes,[38] credit reporting,[39] and the healthcare industry,[40] to name a few examples.[41]

B. The Two Prongs of Section 5

One of the most important and widely used of the FTC's tools is Section 5 of the FTCA, added in 1938, as discussed above, as part of the Wheeler-Lea Amendment.[42]

32. *Our History*, FED. TRADE COMM'N, *supra* note 26.

33. *Beales*, *supra* note 12.

34. *Id.*

35. Press Release, Fed. Trade Comm'n, FTC Announces Results of Compliance Testing of Over 300 Funeral Homes (Feb. 25, 1998), http://www.ftc.gov/news-events/press-releases/1998/02/ftc-announces-results-compliance-testing-over-300-funeral-homes.

36. The regulation of vending machine operators was part of what the FTC dubbed "Project Telesweep, . . . a nationwide federal-state crackdown on business opportunity fraud," which, according to the Commission, "snared nearly 100 marketers of vending machine business opportunities for failure to provide critical pre-purchase information to potential buyers." Press Release, Fed. Trade Comm'n, Four More "Project Telesweep" Defendants Settle FTC Charges (June 5, 1996), http://www.ftc.gov/news-events/press-releases/1996/06/four-more-project-telesweep-defendants-settle-ftc-charges.

37. *See generally, e.g.*, Press Release, Fed. Trade Comm'n, FTC Settlement Requires California Company to Halt Illegal Robocalls (May 14, 2013), http://www.ftc.gov/news-events/press-releases/2013/05/ftc-settlement-requires-california-company-halt-illegal-robocalls.

38. *See generally, e.g.*, Press Release, Fed. Trade Comm'n, Bogus "Rebate" Offers Violate Federal Law (Aug. 5, 2002), http://www.ftc.gov/news-events/press-releases/2002/08/bogus-rebate-offers-violate-federal-law.

39. *See generally, e.g.*, Press Release, Fed. Trade Comm'n, Certegy Check Services to Pay $3.5 Million for Alleged Violations of the Fair Credit Reporting Act and Furnisher Rule (Aug. 15, 2013), http://www.ftc.gov/news-events/press-releases/2013/08/certegy-check-services-pay-35-million-alleged-violations-fair.

40. *See generally, e.g.*, Press Release, Fed. Trade Comm'n, FTC Stops Marketers of Phony Health Care 'Discount' Schemes Directed at Older Americans and Spanish-Speaking Consumers (Sep. 12, 2014), http://www.ftc.gov/news-events/press-releases/2014/09/ftc-stops-marketers-phony-health-care-discount-schemes-directed.

41. "Under the FTC Act, the FTC has broad enforcement authority over large swaths of the economy. For example, the FTC has brought data security actions against retailers, financial institutions, health care-related companies, software and mobile app vendors and, notably, companies that sold products and services relating to data security." Soyong Cho & Andrew L. Caplan, *Cybersecurity Lessons Learned from the FTC's Enforcement History*, K&L GATES LEGAL INSIGHT (K&L Gates LLP, Washington, D.C.), Dec. 2014, at 2.

42. *See supra* note 31 and accompanying text. Section 5 of the FTCA is codified at 15 U.S.C. § 45(a) (2012). According to the Commission, in addition to the FTCA, "the agency also enforces other federal laws

Unlike other specific privacy provisions,[43] Section 5's key language is general (and vague): any "person, partnership, or corporation" is forbidden from engaging in "unfair or deceptive act[s] or practice[s] in or affecting commerce."[44] In other words, Section 5 proscribes two discrete kinds of activity: those that are "deceptive" and those that are, more broadly, "unfair."

Because Congress has granted the FTC authority to interpret the specific provisions of the FTC Act, and because courts generally defer to those interpretations, the Commission has wide latitude to say what kinds of acts or practices are "deceptive" or "unfair."[45] As to the first prong, the FTC proceeded for much of the Act's post-Wheeler-Lea history on the theory that actual deception was not necessary for a deceptiveness claim: it was enough that an act have the potential to deceive "an appreciable or measurable segment of the public," which included "the ignorant, the unthinking and the credulous."[46] But in 1983, the Commission issued a policy statement on deceptiveness, defining the three elements of a deceptiveness claim: "*First*, there must be a representation, omission or practice that is likely to mislead the consumer. . . . *Second*, we examine the practice from the perspective of a consumer acting reasonably in the circumstances. . . . *Third*, the representation, omission, or practice must be a 'material' one."[47] In dissent, two Commissioners argued that this new framework was a hard turn away from the FTC's previous "tendency or capacity" and "credulous consumer" standards.[48]

relating to consumers' privacy and security." *Enforcing Privacy Promises*, FED. TRADE COMM'N, http://www.ftc.gov/news-events/media-resources/protecting-consumer-privacy/enforcing-privacy-promises.

43. *See, e.g.*, 15 U.S.C. § 6801(b) (2012) (directing federal agencies to establish privacy standards "to insure the security and confidentiality of customer records and information," to "protect against any anticipated threats or hazards to the security or integrity of such records," and to "protect against unauthorized access to or use of such records or information which could result in substantial harm or inconvenience to any customer"); 15 U.S.C. §§ 1681c–1681c–2 (2012) (discussing procedures for protecting information contained in credit reports and dealing with identity theft); 15 U.S.C. § 6502(a)(1) (2012) ("It is unlawful for an operator of a website or online service directed to children, or any operator that has actual knowledge that it is collecting personal information from a child, to collect personal information from a child in a manner that violates the regulations prescribed under subsection (b) of this section.").

44. 15 U.S.C. §§ 45(a)(1), (b). *See* Jeff Sovern, *Protecting Privacy with Deceptive Trade Practices Legislation*, 69 FORDHAM L. REV. 1305, 1320 (2001) (citations omitted) ("Though the FTC Act does not mention privacy–it prohibits unfair and deceptive trade practices–it could in fact offer more informational privacy protection than the privacy torts because of the extraordinary scope given its language.").

45. Sovern, *supra* note 44, at 1321.

46. *See* J. Thomas Rosch, Comm'r, Fed. Trade Comm'n, Deceptive and Unfair Acts and Practices Principles: Evolution and Convergence 3 (May 18, 2007) (quoting Feil v. F.T.C., 285 F.2d 879, 892 n.19 (9th Cir. 1960); Aronberg v. F.T.C., 132 F.2d 165, 167 (7th Cir. 1942)).

47. Letter from James C. Miller III, Comm'r, Fed. Trade Comm'n, to John D. Dingel, Chairman, U.S. House of Representatives Comm. on Energy and Commerce (Oct. 14, 1983), https://www.ftc.gov/system/files/documents/public_statements/410531/831014deceptionstmt.pdf.

48. *See* Rosch, *supra* note 46, at 4.

The Commission was quicker to set the contours of the "unfairness" prong, issuing in 1964 a "Statement of Basis and Purpose" which explained the application of Section 5 to cigarette advertisements and set forth three factors the Commission would consider in deciding whether an act or practice was "unfair":

> *(1) whether the practice . . . offends public policy as it has been established by statutes, the common law, or otherwise—whether, in other words, it is within at least the penumbra of some common-law, statutory or other established concept of unfairness; (2) whether it is immoral, unethical, oppressive, or unscrupulous; [and] (3) whether it causes substantial injury to consumers (or competitors or other businessmen).*[49]

Almost a decade later, the Supreme Court gave an approving nod to these three factors in *FTC v. Sperry & Hutchinson Co.*, and appeared to endorse the view that the Commission could deem a practice unfair based on the third prong (substantial injury to consumers) alone.[50]

In 1980, at the request of Congress, the Commission issued a second policy statement clarifying the three factors. With respect to the third factor, whether a practice causes substantial injury to consumers, the Commission explained that monetary harms and unwarranted health and safety risks would be key to determining whether an injury was "substantial," and that the injury "must not be outweighed by any offsetting consumer or competitive benefits," and "must be one which consumers could not reasonably have avoided."[51] In 1994, Congress codified these three factors, incorporating the Commission's cost-benefit balancing test.[52]

C. Experiments in Self-Regulation

Although the FTC had these now well-developed tools for policing business practices and protecting consumers, they were slow to wield them on one of the most important technological and economic developments in United States history: the internet. Of course, the impact of the internet's rise can barely be overstated: the

49. Statement of Basis and Purpose of Trade Regulation Rule 408, Unfair or Deceptive Advertising and Labeling of Cigarettes in Relation to the Health Hazards of Smoking, 29 Fed. Reg. 8324, 8355 (July 2, 1964) [hereinafter *Cigarette Rule Statement*].

50. F.T.C. v. Sperry & Hutchinson Co., 405 U.S. 233, 245 n.5 (1972) (rejecting the argument that "a later portion of [the Cigarette Rule Statement] commits the FTC to the view that misconduct in respect of the third of these criteria is not subject to constraint as 'unfair' absent a concomitant showing of misconduct according to the first or second of these criteria").

51. Policy Statement, Fed. Trade Comm'n, FTC Policy Statement on Unfairness (Dec. 17, 1980), https://www.ftc.gov/public-statements/1980/12/ftc-policy-statement-unfairness [hereinafter 1980 Policy Statement, Fed. Trade Comm'n].

52. 15 U.S.C. § 45(n) (2012); *see generally* Beales, *supra* note 12 (discussing the three elements of modern unfairness).

quickly expanding online marketplace provided exciting business opportunities, but also "serv[ed] as a source of vast amounts of personal information about consumers, including children."[53] Important information, Americans were starting to realize, was often frighteningly insecure in cyberspace. Large-scale cyber-attacks were already making headlines in 1994, the year Congress codified the three "unfairness" factors, with Russian hackers infiltrating Citibank's computer system and siphoning more than $10 million into various international bank accounts.[54]

As cybersecurity was becoming a bigger problem, the FTC might not have been acting quickly to impose new regulations, but they were paying close attention. In 1998, after three years of workshops and hearings, the Commission issued a 63-page report on cybersecurity to Congress.[55] Although the Commission was dismayed at the privacy practices of corporate America, warning that "*substantially greater incentives* are needed," it recommended that appropriate privacy standards could be maintained through self-regulation.[56] The Report did, however, include a list of "fair information practice principles," or FIPPs, it would like to see adopted by the private sector: specifically: (1) notice/awareness ("[c]onsumers should be given notice of an entity's information practices before any personal information is collected from them"); (2) choice/consent ("choice means giving consumers options as to how any personal information collected from them may be used"); (3) access/participation ("refers to an individual's ability both to access data about him or herself . . . and to contest that data's accuracy and completeness"); (4) integrity/security ("The fourth widely accepted principle is that data be accurate

53. FED. TRADE COMM'N, PRIVACY ONLINE: A REPORT TO CONGRESS, at i (1998), https://www.ftc.gov/sites/default/files/documents/reports/privacy-online-report-congress/priv-23a.pdf [hereinafter 1998 Report, FED. TRADE COMM'N].

54. The Citibank case was one of the first of its kind to make news, but not likely the first massive breach. *See* Amy Harmon, *Hacking Theft of $10 Million From Citibank Revealed*, L.A. TIMES (Aug. 19, 1995), http://articles.latimes.com/1995-08-19/business/fi-36656_1_citibank-system ("The incident underscores the vulnerability of financial institutions as they come to increasingly rely on electronic transactions. But computer security experts say what is even more notable about the case is that it became public . . . . Schultz estimates that nearly three dozen cases of computer intruders stealing sums of more than $1 million occur each year in Europe and the United States.").

55. *See generally* 1998 Report, FED. TRADE COMM'N, *supra* note 53.

56. *Id.* at 41; *see also* Daniel J. Solove & Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, 114 COLUM. L. REV. 583, 598–99 (2014) ("Instead of the FTC creating rules, the companies themselves would create their own rules, and the FTC would enforce them. The FTC thus would serve as the backstop to the self-regulatory regime, providing it with oversight and enforcement—essentially, with enough teeth to give it legitimacy and ensure that people would view privacy policies as meaningful and trustworthy."). Although the 1998 Report suggests allowing more time for self-regulation to develop, the Commission called for legislation protecting children's information immediately. 1998 Report, FED. TRADE COMM'N, *supra* note 53, at iii ("In the specific area of children's online privacy, however, the Commission now recommends that Congress develop legislation placing parents in control of the online collection and use of personal information from their children."). COPPA was signed into law the following October. Children's Online Privacy Protection Act, 15 U.S.C. §§ 6501–6506 (2012).

and secure"); and (5) enforcement/redress ("the core principles of privacy protection can only be effective if there is a mechanism in place to enforce them").[57]

The Report stated that "[t]he Commission has encouraged industry to address consumer concerns regarding online privacy through self-regulation," and that "[e]ffective self-regulation remains desirable because it allows firms to respond quickly to technological changes and employ new technologies to protect consumer privacy."[58] In 1999, the Committee issued a second report recommending that self-regulation be given more time, finding "notable progress" by companies in the privacy arena, and citing surveys that showed sixty-six percent of the websites post "at least one disclosure about their information practices," while "forty-four percent of these sites post privacy policy notices."[59]

Although the FTC remained generally sanguine about self-regulation, it was also dipping its toe into the cybersecurity waters, settling its first "internet privacy case" against web hosting company GeoCities in 1998.[60] In the FTC's earliest Section 5 cybersecurity cases, including GeoCities, the FTC's accusations were limited efforts to go after companies that had violated their own privacy policies under Section 5's "deceptiveness" prong.[61]

To the Commission's dismay, as internet commerce continued to grow and consumers' privacy concerns heightened, these two pillars of its strategy (promoting self-regulation and prosecuting deceptiveness cases) eventually began to prove

57. 1998 Report, FED. TRADE COMM'N, *supra* note 53, at 7–10; F.T.C. v. LabMD*: FTC Jurisdiction Over Information Privacy is Plausible, But How Far Can It Go?*, 62 AMER. U. L. REV. 1401, 1407 (2013) ("The detractors assert that 'extensive, yet vaguely phrased, privacy requirements' constitute a 'blank check' to the FTC or any other agency. Others have argued that the Report relies too heavily on FIPPs, which in turn relies heavily on reasonability.").

58. 1998 Report, FED. TRADE COMM'N, *supra* note 53, at 41.

59. Fed. Trade Comm'n, Prepared Statement of the Federal Trade Commission on "Self-Regulation and Privacy Online," Address Before the United States Senate Subcommittee on Communications of the Committee on Commerce, Science, and Transportation 4–5 (July 13, 1999), https://www.ftc.gov/sites/default/files/documents/public_statements/prepared-statement-federal-trade-commission-self-regulation-and-privacy-online/privacyonlinetestimony.pdf.

60. *See* Press Release, Fed. Trade Comm'n, Internet Site Agrees to Settle FTC Charges of Deceptively Collecting Personal Information in Agency's First Internet Privacy Case (Aug. 13, 1998), http://www.ftc.gov/news-events/press-releases/1998/08/internet-site-agrees-settle-ftc-charges-deceptively-collecting; *see also* GINA STEVENS, CONG. RESEARCH SERV., THE FEDERAL TRADE COMMISSION'S REGULATION OF DATA SECURITY UNDER ITS UNFAIR OR DECEPTIVE ACTS OR PRACTICES (UDAP) AUTHORITY, (2014), https://fas.org/sgp/crs/misc/R43723.pdf [hereinafter STEVENS, CONG. RESEARCH SERV.] ("In 1995, the FTC first became involved with consumer privacy issues. Initially, the FTC promoted industry self-regulation as the preferred approach to combatting threats to consumer privacy. After assessing its effectiveness, however, the FTC reported to Congress that self-regulation was not working. Thereupon, the FTC began taking legal action under Section 5 of the FTC Act.").

61. Michael D. Scott, *The FTC, The Unfairness Doctrine, and Data Security Breach Litigation: Has the Commission Gone Too Far?*, 60 ADMIN. L. REV. 127, 131–32, 133 n.40 (2008); Even where FTC complaints mentioned unfairness, the focus was still on deceptiveness. *Id.* at 134.

inadequate.[62] Self-regulation was failing to keep pace with the rapidly growing and changing marketplace, at least to the Commission's satisfaction, and the deceptiveness prong of Section 5, which always focused on the "deceptiveness of the targeted practices" was of limited value against entities with no privacy policy at all, or entities with privacy policies that accurately spelled out inadequate information security practices.[63] In its various reports, you can see the FTC becoming increasingly frustrated and uneasy with the state of cybersecurity in the newly connected world. In a second report on cybersecurity released in 2000, just two years after its first report, the FTC applauded "the significant efforts of the private sector and commends industry leaders in developing self-regulatory initiatives," but concluded that "industry efforts alone have not been sufficient"[64] and called on Congress to enact comprehensive privacy legislation based on the "fair information practice principles" first laid out in 1998.[65]

Although the FTC has since taken the lead in setting cybersecurity standards, developing something like a body of common law with its vast collection of complaints, privacy guides, and consent decrees, it has continued to push Congress to enact broad cybersecurity legislation. In 2010 and 2012, in its most recent cybersecurity reports, the FTC reissued its calls for legislation based on the FIPPs.[66]

62. *See* 2000 Report, FED. TRADE COMM'N, *supra* note 14, at 1 ("Over the past five years, the Internet has changed dramatically from a large network of computers that touched the lives of few consumers to a new marketplace where millions of consumers shop for information, purchase goods and services, and participate in discussions. The technological developments that have made e-commerce possible also have enhanced the ability of companies to collect, store, transfer, and analyze vast amounts of data from and about the consumers who visit their sites on the World Wide Web. This increase in the collection and use of data, along with the myriad subsequent uses of this information that interactive technology makes possible, has raised public awareness and increased concern about online consumer privacy.").

63. *See* Scott, *supra* note 61, at 130, 133, 133 n.41, 11; *see also* Beales, *supra* note 12 ("Unfortunately, the pendulum swung too far the other way and, in the 1990's, the Commission almost entirely avoided the use of unfairness. It became the theory of last resort. Now, however, the FTC is using unfairness to attack practices that cause substantial injury, but that could not be reached under deception theory - at least not without twisting the meaning of deception.").

64. 2000 Report, FED. TRADE COMM'N, *supra* note 14, at ii. Even in the 1998 Report, it was evident the FTC was getting impatient. *See* 1998 Report, FED. TRADE COMM'N, *supra* note 53, at 41 ("To date . . . the Commission has not seen an effective self-regulatory system emerge. As evidenced by the Commission's survey results, and despite the Commission's three-year privacy initiative supporting a self-regulatory response to consumers' privacy concerns, the vast majority of online businesses have yet to adopt even the most fundamental fair information practice (notice/awareness.)").

65. *See* 2000 Report, FED. TRADE COMM'N, *supra* note 14, at 36 ("Ongoing consumer concerns regarding privacy online and the limited success of self-regulatory efforts to date make it time for government to act to protect consumers privacy on the Internet.").

66. *See generally* FED. TRADE COMM'N, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE: A PROPOSED FRAMEWORK FOR BUSINESSES AND POLICYMAKERS (2010), https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-bureau-consumer-protection-preliminary-ftc-staff-report-protecting-consumer/101201privacyreport.pdf [hereinafter 2010 Report, FED. TRADE COMM'N]; FED. TRADE COMM'N, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE: A PROPOSED FRAMEWORK FOR

In these reports, the Commission also introduced and developed, for the first time, the concept of "Privacy by Design" ("PbD"), which businesses can implement by "building privacy protections into their everyday business practices."[67] The Commission explained that "privacy by design" protections include "providing reasonable security for consumer data, collecting only the data needed for a specific business purpose, retaining data only as long as necessary to fulfill that purpose, safely disposing of data no longer being used, and implementing reasonable procedures to promote data accuracy."[68]

So far, Congress has not answered the Commission's call for broader legislation, but it has, at various times, enacted narrower laws aimed at securing specific types of online and other data, including the Children's Online Privacy Protection Act ("COPPA"),[69] which applies to the personal information of children under 13, the Fair Credit Reporting Act ("FCRA"),[70] which applies to information collected by consumer reporting agencies, and the Gramm-Leach-Bliley Act ("GLBA"),[71] which requires financial institutions to disclose information sharing practices.

D. A De Facto Cybersecurity Agency

In the continued absence of a comprehensive statute,[72] the FTC, left alone to police the vast number of data practices not covered by specific internet privacy legislation, has increasingly begun to apply the "unfairness" prong of Section 5 to

BUSINESSES AND POLICYMAKERS (2012), https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf [hereinafter 2012 Report, FED. TRADE COMM'N]. For an extended discussion of Privacy by Design, see *infra* Section IV.

67. 2010 Report, FED. TRADE COMM'N, *supra* note 66, at v.

68. *Id.* at v, 44.

69. Children's Online Privacy Protection Act, 15 U.S.C. §§ 6501–6506 (2012). COPPA is designed to put parents in control over what information can be collected from children online, and applies to minors under the age of 13. *Id.*; *see also Complying with COPPA: Frequently Asked Questions*, FED. TRADE COMM'N (Mar. 2015), https://www.ftc.gov/tips-advice/business-center/guidance/complying-coppa-frequently-asked-questions. The text of COPPA directed the FTC to promulgate specific regulations governing the collection of data from minors under 13, the result of which was the COPPA Rule, which went into effect on April 21, 2000. *See id.*; 15 U.S.C. § 6502 (2012).

70. Fair Credit Reporting Act, 15 U.S.C. § 1681 (2012); *see also Fair Credit Reporting Act*, FED. TRADE COMM'N, https://www.ftc.gov/enforcement/statutes/fair-credit-reporting-act (last visited Feb. 14, 2017).

71. 15 U.S.C. §§ 6801–6827 (1999).

72. That absence continues; most notably, the Cyber Security Act has stalled more than once in Congress. *See, e.g.*, Michael S. Schmidt, *Cybersecurity Bill is Blocked in Senate by G.O.P. Filibuster*, N.Y. TIMES (Aug. 2, 2012), http://www.nytimes.com/2012/08/03/us/politics/cybersecurity-bill-blocked-by-gop-filibuster.html. In February, 2012, President Obama first proposed a "Consumer Privacy Bill of Rights," incorporating the FIPPs. Andrew Lustigman & Adam Solomon, *An Overview and the Impact of the Consumer Privacy Bill of Rights*, INSIDE COUNSEL (Mar. 12, 2015), http://www.insidecounsel.com/2015/03/12/an-overview-and-the-impact-of-the-consumer-privacy. The bill was reintroduced in February 2015. *Id.*

data security cases.[73] Since its first case against GeoCities in 1998, the FTC has filed almost 200 privacy cases,[74] and since 2005, the Commission has cited the unfairness doctrine in almost 30 data security cases.[75] Approximately 20 of these "unfairness" cases have been filed since 2011.[76] In the majority of these cases, the respondent has suffered a security breach,[77] and the FTC files an administrative complaint[78] in which it (1) alleges that "respondent engaged in a number of practices that, taken together, failed to provide reasonable and appropriate security" for personal information, (2) lists the specific data security practices that were insufficient, and (3) argues that "respondent's failure to employ reasonable and appropriate security measures to protect personal information caused or is likely to cause substantial injury to consumers that is not offset by countervailing benefits to consumers or competition and is not reasonably avoidable by consumers."[79]

73. *See* Serwin, *supra* note 28, at 815, 816 (discussing the FTC's shift from a "notice-and-choice" model of enforcement, which was focused on giving consumers informed choices about privacy, and the "harm-based model," which focuses instead on whether the consumer suffered harm). "[T]he harm-based approach, represented a departure from the notice-and-choice model. Although the FTC continued to use deception in its cases, later cases focused more on actual consumer injury—typically resulting from an alleged breach—and the FTC began instead to rely more on its unfairness authority." *Id.* at 816.

74. *See Legal Resources*, FED. TRADE COMM'N, https://www.ftc.gov/tips-advice/business-center/legal-resources (selecting type: "Case," and topic: "Privacy and Security" will cull the site to these relevant cases); *see also* Solove & Hartzog, *supra* note 56 at 600 (citations omitted) ("[T]hat number is slightly misleading given the steady increase in annual complaints. For example, the FTC brought nine privacy-related complaints in 2002, compared to 2012, in which it brought twenty-four complaints for unique privacy-related violations."); Cho & Caplan, *supra* note 41 ("Since 2002, the FTC has brought nearly 60 data security enforcement matters and settled more than 50 of those actions. The FTC's data security activity has accelerated in recent years and likely will continue to do so.").

75. FED. TRADE COMM'N, PRIVACY & DATA SECURITY UPDATE (2015), https://www.ftc.gov/reports/privacy-data-security-update-2015.

76. *See Legal Resources*, FED. TRADE COMM'N, supra note 74 (offering a database of sortable FTC case, which can be filtered to relevant "Data Security" cases, through the "Topic" toggle). This filtering will still not include cases where the Commission invokes the text of Section 5, including the unfairness prong, but cases in which the complaint is exclusively focused on deception. *See generally, e.g.*, Complaint, *In re* Superior Mortg. Corp., 140 F.T.C. 926 (Dec. 16, 2005). For a case only focusing on the unfairness prong, or cases in which both prongs were invoked meaningfully, see generally Complaint, *In re* Ceridian Corp., 151 F.T.C. 514 (June 15, 2011).

77. For an example of an FTC filing that did not involve a "breach" concerning a malicious outsider seeking access to company data, see Complaint at 2–3, *In re* Rite Aid Corp., 150 F.T.C. 694 (2010) (alleging disposal of documents with personal information in clearly readable text, such as pharmacy labels and employment applications, in a dumpster).

78. Occasionally, the FTC, rather than filing an administrative complaint, files a complaint in federal court to enforce Section 5. *See generally, e.g.*, Complaint, United States v. Rental Res. Servs., Inc., 10 F. Supp. 3d 602 (D. N.J. Mar. 5, 2009) (No. 13-8887); *Wyndham Complaint*, *supra* note 2.

79. Complaint at 2–3, *In re* Dave & Buster's, Inc., 149 F.T.C. 1449 (2011); *see also In re* ACRAnet, Inc., F.T.C. (2011) (No. C-4331). In 2007, the Commission issued a guidebook, which included a "checklist" for a "sound data security plan." *Protecting Personal Information: A Guide for Business*, FED. TRADE COMM'N (2016) [hereinafter *FTC Guidebook*].

The Commission's data security investigations have targeted companies as high profile as Microsoft,[80] Google,[81] Facebook,[82] Twitter,[83] Snapchat,[84] and HTC.[85] In addition to having authority over privacy matters under specific statutes—such as the GLBA,[86] COPPA,[87] the FCRA[88]— as well as under Privacy Shield, an agreement between the U.S. and the European Union governing transatlantic data flows,[89] and under the deceptiveness prong of Section 5 of the FTCA,[90] the Commission has widely applied the unfairness doctrine to data security cases as well.[91] Now, the FTC can bring an enforcement action not only for a company's failure to adhere to its privacy policy, but for any "unfair" act or practice.[92] "This fact has effectively given the FTC a sprawling jurisdiction to enforce privacy in addition to the pockets of

80. *See generally In re* Microsoft Corp., 131 F.T.C. 1113 (2015); Press Release, Fed. Trade Comm'n, Microsoft Settles FTC Charges Alleging False Security and Privacy Promises (Aug. 8, 2002), https://www.ftc.gov/news-events/press-releases/2002/08/microsoft-settles-ftc-charges-alleging-false-security-privacy.

81. *See generally* Complaint, *In re* Google, Inc., (No. C-4336), 2014 WL 6984156 (2014); Press Release, Fed. Trade. Comm'n, Google Will Pay $22.5 Million to Settle FTC Charges it Misrepresented Privacy Assurances to Users of Apple's Safari Internet Browser (Aug. 9, 2012), https://www.ftc.gov/news-events/press-releases/2012/08/google-will-pay-225-million-settle-ftc-charges-it-misrepresented.

82. *See generally* Complaint, *In re* Facebook, Inc., (No. C-4365), 2012 WL 3518628 (2012); Press Release, Fed. Trade Comm'n, FTC Approves Final Settlement With Facebook (Aug. 10, 2012), https://www.ftc.gov/news-events/press-releases/2012/08/ftc-approves-final-settlement-facebook.

83. *See generally* Complaint, *In re* Twitter, Inc., 151 F.T.C. 162 (2011); Press Release, Fed. Trade Comm'n, FTC Accepts Final Settlement with Twitter for Failure to Safeguard Personal Information (Mar. 11, 2011), https://www.ftc.gov/news-events/press-releases/2011/03/ftc-accepts-final-settlement-twitter-failure-safeguard-personal-0.

84. *See generally* Complaint, *In re* Snapchat, Inc., 2014 WL 7495798 (2014); Press Release, Fed. Trade Comm'n, Snapchat Settles FTC Charges That Promises of Disappearing Messages Were False (May 8, 2014), https://www.ftc.gov/news-events/press-releases/2014/05/snapchat-settles-ftc-charges-promises-disappearing-messages-were.

85. *See generally* Complaint, *In re* HTC America, Inc., 155 F.T.C. 1617 (2013); Press Release, Fed. Trade Comm'n, HTC America Settles FTC Charges It Failed to Secure Millions of Mobile Devices Shipped to Consumers (Feb. 22, 2013), https://www.ftc.gov/news-events/press-releases/2013/02/htc-america-settles-ftc-charges-it-failed-secure-millions-mobile.

86. *See supra* note 71 and accompanying text.

87. *See supra* note 69 and accompanying text.

88. *See supra* note 70 and accompanying text.

89. *See Privacy Shield Overview*, INTERNATIONAL TRADE ADMINISTRATION, https://www.privacyshield.gov/Program-Overview. Implemented in early 2016, Privacy Shield replaces the Safe Harbor Framework, struck down in 2015 by a European Court following revelations by NSA whistleblower Edward Snowden about U.S. government surveillance practices. *See* Sebastian Anthony, *Europe's Highest Court Strikes Down Safe Harbor Data Sharing Between EU, US*, ARS TECHNICA (Oct. 6, 2015), https://arstechnica.com/tech-policy/2015/10/europes-highest-court-strikes-down-safe-harbour-data-sharing-between-eu-and-us.

90. *See* Solove & Hartzog, *supra* note 56, at 598.

91. STEVENS, CONG. RESEARCH SERV., *supra* note 60.

92. *See* Solove & Hartzog, *supra* note 56, at 588.

statutory jurisdiction Congress has given to it in industry-specific privacy legislation. The FTC reigns over more territory than any other agency that deals with privacy."[93] Moreover, the cost of coming under FTC scrutiny is significant: in addition to the expense of complying with an FTC investigation, consent decrees in data privacy cases contain financial penalties, and reporting, audit, and compliance requirements which may last up to 20 years.[94]

After almost 20 years of investigating and enforcing internet privacy, the Commission has prosecuted a significant number of data security cases, and in those cases evolved a set of privacy principles. One commentator has even likened the FTC's consent decrees to a body of common law: the implication is that the Commission, in addition to its investigatory role, has become a kind of national privacy court, whose case archives companies and individuals comb for applicable principles and best practices.[95] Regardless of whether, as some argue, the FTC is a weak privacy regulator,[96] the commission is unrivaled in the privacy arena, and, far from pursuing the passive, self-regulatory approach of the mid-nineties, has emerged as the leading arbiter of what constitutes reasonable data security.[97]

93. *Id.*

94. *Id.* at 613–14. Generally, an FTC cybersecurity case proceeds in two stages: investigation and enforcement. *See A Brief Overview of the Federal Trade Commission's Investigative and Law Enforcement Authority*, FED. TRADE COMM'N (July 2008), https://www.ftc.gov/about-ftc/what-we-do/enforcement-authority [hereinafter FTC Overview, FED. TRADE COMM'N]. The investigative stage may include an informal investigation, initially. But formally, the investigation stage typically begins with the FTC filing a "civil investigative demand" ("CID"), which may require that companies produce documents and oral testimony, in addition to written reports or answers to questions. *Id.* The FTC may petition a federal court to enforce the CID, in the event of noncompliance. *Id.* Following an investigation, the FTC may initiate an enforcement action if it has "reason to believe" that the law has been violated. *Id.* Typically in cybersecurity cases, the FTC initiates an administrative enforcement by filing an administrative complaint. *Id.* If a party wishes to settle the case, it may sign a consent agreement, which may include financial penalties, as well as compliance requirements. *Id.* If the party wishes to seek administrative review, the case is adjudicated before an administrative law judge ("ALJ"), who issues a final order on the case. *Id.* In addition to administrative proceedings, the FTC may seek enforcement of consent decrees, or of an ALJ's order, in federal court. *Id.*

95. For the FTC's own summary of the principles in its own cybersecurity cases, see *Start with Security: Lessons Learned from FTC Cases*, FED. TRADE COMM'N (June 2015), https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf [hereinafter *Start with Security*].

96. *See, e.g.*, Peter Maass, *Your FTC Privacy Watchdogs: Low-Tech, Defensive, Toothless*, WIRED (June 28, 2012), http://www.wired.com/2012/06/ftc-fail/all.

97. *See* Steven Hetcher, *The FTC as Internet Privacy Norm Entrepreneur*, 53 VAND. L. REV. 2041, 2053, 2062 (2000) ("While the Agency has seemed to promote industry self-regulation, it has all the while been establishing the predicate for its jurisdictional grasp over website activities. Because the FTC is able to gain a jurisdictional foothold by means of promoting more respected website privacy norms, the Agency is aptly characterized as a privacy norm entrepreneur."); Solove & Hartzog, *supra* note 56, at 600 ("Today, the FTC is viewed as the de facto federal data protection authority. A data protection authority is common in the privacy law of most other countries, which designate a particular agency to have the power to enforce privacy laws. Critics of the FTC call it weak and ineffective . . . . But many privacy lawyers and companies view the FTC as a formidable enforcement power, and they closely scrutinize FTC actions in order to guide their decisions" (quoting Maass, *supra* note

Although the FTC's expanded use of the "unfairness doctrine" is not without precedent in other areas of law,[98] critics argue (among other things) that a data security breach does not constitute substantial injury to consumers,[99] that the "unfairness" prong is too broadly applied,[100] and that the FTC has been granted sufficient authority in other specific statutes to police data security.[101] Because most of the cases where the FTC has pressed an unfairness argument have settled, the Commission has been free to prosecute cybersecurity cases under the "unfairness" prong.

96)); Christopher Matthews, *Wyndham, FTC Clash on Cybersercurity*, WALL ST. J. (Nov. 7, 2013), http://www.wsj.com/articles/SB10001424052702304672404579184291131616548 ("Congress has yet to give any Washington agency explicit authority to regulate corporate cybersecurity in general or order companies to beef up the security of their systems. So, the FTC has stepped into the breach, citing its long-standing power to protect consumers."); Paul Rosenzweig, *Which Federal Agency Controls Cybersecurity? The Answer May Surprise You*, THE NEW REPUBLIC (Apr. 16, 2014), http://www.newrepublic.com/article/117389/ftc-gains-control-cybersecurity-measures-after-wyndham-hotels -case ("The FTC has a legal hammer, and we can expect the agency to use it.").

98. The FTC's Policy Statement on Unfairness, delivered to Congress in 1980, argues for an expansive interpretation of Section 5:

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

1980 Policy Statement, Fed Trade Comm'n, *supra* note 51. Since the Commission's 1980 Policy Statement, the FTC's use of the unfairness doctrine has expanded, contracted, and is now seeing a revival. *See* Beales, *supra* note 12 ("Unfortunately, the pendulum swung too far the other way and, in the 1990's, the Commission almost entirely avoided the use of unfairness. It became the theory of last resort. Now, however, the FTC is using unfairness to attack practices that cause substantial injury, but that could not be reached under deception theory - at least not without twisting the meaning of deception."). Note, however, that the FTC is not the only regulator in the cybersecurity game. Private plaintiffs and state authorities are also important checks and regulators of cybersecurity. *See* Alan Charles Raul, et al., *United States, in* THE PRIVACY, DATA PROTECTION AND CYBERSECURITY LAW REVIEW 268, 272 (2014). In 2014, the Federal Communications Commission ("FCC") reached a $10 million settlement with two telecommunications companies in the wake of 2012 and 2013 cybersecurity breaches, the FCC's first cybersecurity settlement. Tom Risen, *FCC Adds Cybersecurity to Its Oversight*, U.S. NEWS (Oct. 24, 2014), http://www.usnews.com/news/articles/2014/10/24/fcc-adds-cybersecurity-to-its-oversight. In 2016, the Consumer Financial Protection Bureau ("CFPB") announced its first cybersecurity settlement, with Dwolla, Inc., a digital payment platform that permits real-time bank transfers, and in so doing collects sensitive personal information. *See* Ryan M. Martin & Liisa M. Thomas, *U.S. Consumer Financial Protection Bureau Announces Its First Privacy Settlement*, WINSTON & STRAWN LLP, (Mar. 15, 2016), http://www.lexology.com/library/detail.aspx?g=6f24b842-8dfa-45c0-b13e-bba0b79b3505. The consent order required Dwolla to pay a penalty of $100,000 to the CFPB, in addition to other compliance requirements. *Id.*

99. *See* Scott, *supra* note 61, at 32.

100. *See, e.g.*, Michael Chertoff, *The Lessons of Google's Safari Hack*, WALL ST. J. (Jul. 22, 2012), http://www.wsj.com/articles/SB10001424052702303933704577532572854142492 ("Using consumer-protection laws to address cyber vulnerabilities is stretching the FTC's mission beyond recognition.").

101. Raul, et al., *supra* note 98, at 272.

As discussed below, the Wyndham and LabMD cases represent the first significant legal challenges to the FTC's "unfairness" approach, and the Third Circuit's opinion in *Wyndham* is, perhaps, the first sign that the FTC will get the federal judiciary's blessing to continue its broadened efforts to police data security on the basis of unfairness.

III. WYNDHAM AND LABMD PUSH BACK

A. In the Matter of LabMD

Atlanta-based LabMD, Inc., was "in the business of conducting clinical laboratory tests on specimen samples from consumers and reporting test results to consumers' health care providers."[102] After conducting the tests, LabMD collected payment for the tests from consumers' health insurance companies, from consumers directly, or both.[103] In performing the tests, and to facilitate payment, LabMD collected information about consumers, including patients' Social Security Numbers ("SSNs"), medical record numbers, bank account or credit card numbers, and health insurance company names and policy numbers.[104] LabMD had collected such information from nearly one million consumers, and stored the information on a computer network which included computers in LabMD's corporate offices in Georgia, computers used by LabMD personnel in other parts of the country, and computers provided by LabMD to healthcare providers.[105]

In May 2008, cyber-intelligence company Tiversa informed LabMD that a file containing the personal information of approximately 9,300 consumers was available on a peer-to-peer ("P2P") file-sharing network through the file-sharing application Limewire.[106] LabMD subsequently discovered that Limewire had been

102. *LabMD Complaint*, *supra* note 3, at 1.

103. *Id.*

104. *Id.* at 2.

105. *Id.* According to the complaint, LabMD used the computer systems to "receive orders for tests from health care providers; report test results to health care providers; file insurance claims with health insurance companies; prepare bills and other correspondence to consumers; obtain approvals for payments made by consumers with credit cards; and prepare medical records." *Id.* at 2. In so doing, LabMD stored, for example, monthly spreadsheets of insurance claims and payments ("insurance aging reports"), which included consumer names, dates of birth, SSNs, and health insurance company names, addresses, and policy numbers; spreadsheets of payments received from consumers ("day sheets"), which include consumer names, SSNs, and methods, amounts, and dates of payments; and copies of consumer checks, which included names, addresses, telephone numbers, payment amounts, bank names and routing numbers, and bank account numbers ("copied checks"). *Id.*

106. *Id.* at 4. "Peer-to-Peer (P2P) technology is a way to share music, video and documents, play games, and facilitate online telephone conversations. The technology enables computers using the same or compatible P2P programs to form a network and share digital files directly with other computers on the network. Because virtually anyone can join a P2P network just by installing particular software, millions of computers could be connected at one time." *Peer-to-Peer File Sharing: A Guide for Business*, FED. TRADE COMM'N,

installed on a computer in its billing department no later than 2006.[107] In October 2012, Sacramento police found individuals in possession of an "insurance aging file," or "1718 file,"[108] from LabMD, which included "personal information, such as names and SSNs, of several hundred consumers in different states."[109] The FTC conceded in its complaint, filed in August 2013, that "[m]any of these consumers were not included in the P2P insurance aging file, and some of the information post-dates the P2P insurance aging file," but argued that "[a] number of the SSNs in the Day Sheets are being, or have been, used by people with different names, which *may* indicate that the SSNs have been used by identity thieves."[110] The FTC alleged that LabMD:

- did not develop, implement, or maintain a comprehensive security program;[111]
- did not use readily available measures to identify commonly known and foreseeable risks;[112]
- did not prevent employees from unnecessarily accessing personal information;[113]
- did not adequately train employees to safeguard personal information;[114]
- did not require common authentication-related security measures;[115]
- did not maintain and update operating systems of network computers;[116] and

https://www.ftc.gov/es/system/files/documents/plain-language/bus46-peer-peer-file-sharing-guide-business.pdf.

107. *LabMD Complaint*, *supra* note 3, at 4.

108. *Id.* at 4–5. According to the Complaint, the file "contain[ed] personal information about approximately 9,300 consumers, including names, dates of birth, SSNs, CPT codes, and, in many instances, health insurance company names, addresses, and policy numbers." *Id.* at 4.

109. *Id.* at 5.

110. *Id.* (emphasis added).

111. *Id.* at 3. The Commission specifically alleged that "employees were allowed to send emails with such information to their personal email accounts without using readily available measures to protect the information from unauthorized disclosure." *Id.*

112. *LabMD Complaint*, *supra* note 3, at 3. Specifically, the Commission noted LabMD's failure to use "penetration tests." *Id.* In a penetration test, computer systems are purposefully hacked to locate weaknesses and vulnerabilities. *See What is Penetration Testing?*, CORE SECURITY, http://www.coresecurity.com/penetration-testing-overview.

113. *LabMD Complaint*, *supra* note 3, at 3.

114. *Id.*

115. *Id.* "Common authentication-related security measures" specifically mentioned by the Commission include "periodically changing passwords, prohibiting the use of the same password across applications," and using "two-factor authentication" (combining a user name and a password, or a password and a pin, for example). *Id.*

116. *Id.*

- did not employ readily available measures to prevent or detect unauthorized access to computer networks.[117]

According to the Commission, these practices, "taken together, failed to provide reasonable and appropriate security for personal information on its computer networks."[118] The FTC argued that LabMD's deficient security "caused, or is likely to cause, substantial injury to consumers that is not offset by countervailing benefits to consumers or competition and is not reasonably avoidable by consumers. This practice was, and is, an unfair act or practice."[119]

LabMD subsequently filed a motion to dismiss, arguing, among other things, that "Congress has not given the FTC the power to use its Section 5 'unfairness' authority to do what it has done to LabMD here," and that, "even if Section 5 authorized the FTC to broadly regulate data-security practices as 'unfair' acts or practices, [HIPAA] and the Health Information Technology for Economic and Clinical Health Act (HITECH), as interpreted and enforced by HHS, control."[120] The Commission denied the motion.[121] LabMD also filed complaints in the Northern District of Georgia and the District of Columbia seeking to enjoin the agency proceeding, and an emergency motion in the U.S. Eleventh Circuit Court of Appeals.[122] LabMD dropped the action in the District of Columbia and has so far been denied relief in the Northern District of Georgia and at the Eleventh Circuit.[123]

In June 2014, *LabMD* took a bizarre turn when the House Oversight and Government Reform Committee began investigating the FTC's relationship with Tiversa, the cybersecurity firm that alerted LabMD of the security breach and later informed the FTC, leading to the investigation.[124] After Tiversa employees testified

117. *Id.* at 3. The Commission alleged specifically that LabMD "did not use appropriate measures to prevent employees from installing . . . applications or materials that were not needed to perform their jobs," and did not "adequately maintain or review records of activity on its networks." *Id.* "As a result, respondent did not detect the installation or use of an unauthorized file sharing application on its networks." *Id.*

118. *Id.*

119. *LabMD Complaint*, *supra* note 3, at 5.

120. Motion to Dismiss Complaint With Prejudice and to Stay Administrative Proceedings at 3, *In re* LabMD, 2013 WL 5232775 (F.T.C. Nov. 12, 2013) (No. 9357).

121. *See generally* Order Denying Motion to Dismiss, *In re* LabMD, 2013 WL 5232775 (F.T.C. Jan. 16, 2014) (No. 9357), http://www.ftc.gov/sites/default/files/documents/cases/140117labmdorder.pdf.

122. *See* Evan M. Wooten & Lei Shen, *The Curious Case of LabMD New Developments in the "Other" FTC Data-Security Case*, MAYER BROWN LLP (Aug. 11, 2014), http://www.lexology.com/library/detail.aspx?g=8e53bce4-c048-403c-97e5-deecefe844cf (providing an overview of the tortuous procedural history of the *LabMD* case).

123. *See In the Matter of LabMD, Inc.*, FED. TRADE COMM'N (Sept. 29, 2016), https://www.ftc.gov/enforcement/cases-proceedings/102-3099/labmd-inc-matter.

124. Allegedly, after discovering a document containing personal information on Limewire's P2P network, Tiversa alerted LabMD of the security breach, and offered to sell them "remediation" services to shore up security, which services LabMD turned down. *See* Press Release, House Oversight and Government Reform Comm., Issa to FTC Watchdog: Investigate Allegations of Corporate Blackmail (June 18, 2014),

to the Oversight Committee that the information given to the FTC concerning LabMD may have been inaccurate, Oversight Committee Chairman Darrell Issa sent a letter to the Commission's Inspector General ("IG") requesting that the IG's office investigate the FTC's relationship with Tiversa.[125] In May 2014, the Oversight Committee released its own report on Tiversa, concluding that the company had provided incomplete, inconsistent, and/or conflicting information to the FTC.[126] "Instead of acting as the 'white knight' the company purports to be, Tiversa often acted unethically and sometimes unlawfully after downloading documents unintentionally exposed on peer-to-peer networks," the report argues, claiming that Tiversa "routinely provided falsified information to federal government agencies."[127] As discussed below, Tiversa's relationship with the FTC has also taken center stage in LabMD's ongoing administrative proceeding, in what has been framed as part David vs. Goliath struggle and part Kafka-esque nightmare of a small business railroaded by the Leviathan state.[128]

B. FTC v. Wyndham

Wyndham and its subsidiaries[129] license the "Wyndham" name to approximately 90 hotels under either franchise or management agreements.[130] According to these

https://oversight.house.gov/release/issa-ftc-watchdog-investigate-allegations-corporate-blackmail. It is also alleged that, when their services were rejected, Tiversa turned LabMD in to the FTC. *Id.*

125. *See House Oversight Notifies FTC of Investigation Into Tiversa and "Less Than Accurate" Information it Provided in LabMD Case (Update 1)*, DATABREACHES.NET (June 12, 2014), https://www.databreaches.net/house-oversight-notifies-ftc-of-investigation-into-tiversa-and-less-than-accurate-information-it-provided-in-labmd-case; *see also* Grant Gross, *House Panel Investigating Data Breach Enforcement*, COMPUTERWORLD (May 30, 2014), http://www.computerworld.com/article/2490055/cybercrime-hacking/house-panel-investigating-ftc-data-breach-enforcement.html; Brian Mahoney, *LabMD Trial Delayed While House Panel Probes Tiversa*, LAW360 (May 30, 2014), http://www.law360.com/articles/543238/labmd-trial-delayed-while-house-panel-probes-tiversa.

126. *See* Exhibit 1, Respondent LabMD, Inc.'s Unopposed Motion to Refer Tiversa, Inc., Tiversa Holding Corp., and Robert Boback for Investigation Regarding Potential Criminal Violations of 42 U.S.C. § 1320D-6(a), 18 U.S.C. §§ 371, 1001, 1030, 1505, and 1519 at 4, *In re* LabMD, 2013 WL 5232775 (F.T.C. June 19, 2015) (No. 9357), https://www.ftc.gov/system/files/documents/cases/577890.pdf.

127. *Id.* at 5.

128. *See* Kent Hoover, *LabMD CEO Michael Daugherty fights 'The Devil Inside the Beltway,'* THE BUSINESS JOURNALS (Sept. 13, 2013), http://www.bizjournals.com/bizjournals/washingtonbureau/2013/09/13/medical-testing-lab-fights-the-devil.html. In particular, see former LabMD CEO Michael Daugherty's book about his experiences with Tiversa and the FTC. MICHAEL J. DAUGHERTY, THE DEVIL INSIDE THE BELTWAY: THE SHOCKING EXPOSE OF THE US GOVERNMENT'S SURVEILLANCE AND OVERREACH INTO CYBERSECURITY, MEDICINE AND SMALL BUSINESS (Broadland, 2013).

129. The complaint lists Wyndham Worldwide Corporation, Wyndham Hotel Group LLC, Wyndham Hotels and Resorts LLC, and Wyndham Hotel Management. *Wyndham Complaint*, *supra* note 2, at 1. Under Wyndham's business structure, Hotels and Resorts and Hotel Management are subsidiaries of Hotel Group. *Id.* at 4.

agreements, Wyndham-branded hotels are required to purchase and configure computer systems designed for, among other things, handling reservations and payment card transactions.[131] Specifically, each hotel's computer system, known as a "property management system," stores consumers' personal information, "including names, addresses, email addresses, telephone numbers, payment card account numbers, expiration dates, and security codes."[132] The networks of all Wyndham-branded hotels are linked to the company's corporate network, including a "central reservation system" that "coordinates reservations across the Wyndham brand."[133]

Between April 2008 and January 2010, hackers gained access three separate times to Wyndham's network, including Wyndham-branded hotels' individual property management systems, and stole "more than 619,000 payment card account numbers."[134] The payment card numbers were subsequently posted to a domain registered in Russia, and the breaches, according to the FTC, cost consumers "more than $10.6 million in fraud loss."[135] In its complaint, filed in August 2012, the FTC alleged that Wyndham:

- did not limit access between hotel networks and the Internet;[136]
- allowed payment card information to be stored in clear, readable text;[137]
- did not ensure Wyndham-branded hotels implemented adequate security policies and procedures prior to connecting local computers to Wyndham's network;[138]

130. F.T.C. v. Wyndham Worldwide Corp., 10 F. Supp. 3d 602, 608 (D.N.J. 2014) ("Hotels and Resorts licensed the 'Wyndham' name to approximately seventy-five independently-owned hotels under franchise agreements. Similarly, Hotel Management licensed the 'Wyndham' name to approximately fifteen independently-owned hotels under management agreements." (emphasis omitted)).

131. *Id.*

132. *Id.*

133. *Id.* at 608 ("[A]lthough certain Wyndham-branded hotels have their own websites, customers making reservations for these hotels 'are directed back to Hotels and Resorts' website to make reservations.").

134. *Id.* at 609. In the first attack, occurring in April, 2008, on a local hotel in Phoenix, hackers used "brute force" attack where hackers use computer programs to systematically guess all possible passwords. *Wyndham Complaint*, *supra* note 2, at 13. The first hack resulted in the compromise of 500,000 payment card numbers, which were exported to a domain in Russia. *Id.* at 15. The second attack occurred in March 2009, when hackers gained access through a service provider's administrator account in the company's data center in Phoenix. *Id.* The second hack resulted in the compromise of 50,000 customer payment cards. *Id.* at 16. The third attack occurred in late 2009; hackers again gained access to Wyndham's networks through a service provider administrator's account. *Id.* The breach resulted in the compromise of 69,000 payment card accounts. *Id.* at 16–17.

135. *Wyndham Worldwide Corp.*, 10 F. Supp. 3d at 609.

136. First Amended Complaint for Injunctive and Other Equitable Relief at 10, F.T.C. v. Wyndham Worldwide Corp., 10 F. Supp. 3d 602 (D.N.J. 2014) (No. CV 12-1365-PHX-PGR).

137. *Id.*

- did not remedy known vulnerabilities on hotel servers;[139]
- allowed servers to connect to Wyndham's network, despite the fact that well-known default user IDs and passwords were enabled on the servers;[140]
- did not employ common user ID and password security measures;[141]
- did not adequately inventory computers connected to Wyndham's network;[142]
- did not employ reasonable measures to detect and prevent unauthorized access;[143]
- did not follow proper incident response procedures;[144] and
- did not adequately restrict third-party vendors' access to the network.[145]

According to the Commission, these practices, "taken together, unreasonably and unnecessarily exposed consumers' personal data to unauthorized access and theft."[146] On the basis of these alleged failures, the FTC argued Wyndham's actions "caused or are likely to cause substantial injury to consumers that consumers cannot reasonably avoid themselves and that is not outweighed by countervailing benefits to consumers or competition," and therefore constituted unfair acts under Section 5.[147] The Commission asked the court for (1) a permanent injunction to prevent future violations, (2) "such relief as the Court finds necessary to redress injury to consumers resulting from Defendants' violations of the FTCA, including but not limited to, rescission or reformation of contracts, restitution, the refund of

138. *Id.* at 10–11.

139. *Id.* at 11.

140. *Id.*

141. *Wyndham Complaint*, *supra* note 2, at 11.

142. *Id.* at 11.

143. *Id.* at 12.

144. *Id.*

145. *Id.*

146. *Id.* at 10.

147. *Wyndham Complaint*, *supra* note 2, at 19. Unlike in *LabMD*, discussed below, the FTC also alleged Wyndham violated the deceptiveness prong. *See infra* Section III.E. The portion of Wyndham's privacy policy the FTC considered deceptive, and included in the First Amended Complaint, stated, notably:

> We safeguard our Customers' personally identifiable information by using standard industry practices. Although "guaranteed security" does not exist on or off the Internet, we take commercially reasonable efforts to create and maintain "fire walls" and other appropriate safeguards to ensure that to the extent we control the Information, the Information is used only as authorized by us and consistent with this Policy, and that the Information is not improperly altered or destroyed.

Wyndham Complaint, *supra* note 2, at 9 (replicating langauge from the "Hotel and Resorts'" website, but not providing a specific citation to the quoted language).

monies paid, and the disgorgement of ill-gotten monies"; and (3) the FTC's litigation costs.[148]

Wyndham subsequently filed a motion to dismiss, arguing, among other things, that Congress has, in statutes like the FCRA, the GLBA, and COPPA, granted the FTC authority to regulate data security standards, "but *only* in certain specific, limited contexts," and that these statutes "are powerful evidence that the FTC lacks authority to regulate data-security practices in cases (like this one) that fall outside the confines of those narrow delegations."[149] The District Court denied Wyndham's motion, concluding that "subsequent data-security legislation seems to complement—*not preclude*—the FTC's authority," and that "the FTC's unfairness authority over data security can coexist with the existing data-security regulatory scheme."[150] Wyndham subsequently appealed.[151]

C. Wyndham *at the Third Circuit*

In March of 2015, the U.S. Third Circuit Court of Appeals heard oral argument in the *Wyndham* case, and in August the court issued its opinion.[152] Two questions were before the court: (1) "[W]hether the FTC has authority to regulate cybersecurity under the unfairness prong of [Section 5]; and, if so, (2) whether Wyndham had fair notice its specific cybersecurity practices could fall short of that provision."[153]

1. The FTC's Unfairness Authority

First, the court rejected Wyndham's argument that conduct is only unfair when it injures consumers "through unscrupulous or unethical behavior," noting that the Supreme Court in *Sperry & Hutchinson* had rejected the view that all three factors from the FTC's policy statement are necessary to a showing of "unfairness," and the third factor, whether the act causes substantial injury to consumers, is sufficient for a finding of unfairness.[154]

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

149. Motion to Dismiss at 9, F.T.C. v. Wyndham Worldwide Corp. et al., 2012 WL 3916987 (D. Ariz. Aug. 27, 2012) (No. 12-1365) [hereinafter *Wyndham Motion to Dismiss*].

150. F.T.C. v. Wyndham Worldwide Corp., 10 F. Supp. 3d 602, 613 (D.N.J. 2014).

151. F.T.C. v. Wyndham Worldwide Corp. (*Wyndham II*), 799 F.3d 236, 236 (3d Cir. 2015).

152. *Id.* at 259 (concluding that Wyndham failed to successfully challenge the FTC's claim).

153. *Id.* at 240. The Court noted that Wyndham also argued in its brief that the FTC failed the pleading requirements of an unfairness claim, but declined to address the question, since interlocutory appeal was not granted on the issue. *Id.* at 240 n.1.

154. *Id.* at 244–45; *see also* Brief of Petitioner-Appellant at 20–21, F.T.C. v. Wyndham Worldwide Corp. 799 F.3d 236 (3d Cir. 2015) (No. 14-3514), 2014 WL 5106183 (C.A.3) [hereinafter *Wyndham Opening App. Brief*]; *Cigarette Rule Statement*, *supra* note 49, at 8355.

Next, the court took up Wyndham's argument that the plain meaning of the word "unfair" requires that the FTC take into account more than whether an act or practice causes substantial injury to consumers.[155] Citing the Webster's Dictionary definition of "unfair" ("marked by injustice, partiality, or deception"), Wyndham argued in its opening brief that "[a] business treats consumers 'unfairly,'" not when it simply causes harm, but "when it seeks to take advantage of [customers], or otherwise injures them through unscrupulous or unethical behavior."[156] Wyndham also argued that "[a]s a matter of law and logic, a business does not treat its customers in an 'unfair' manner when the business *itself* is victimized by criminals."[157]

The court's rejection of the latter argument was straightforward, drawing on tort principles to explain that a company may be held accountable for negligent behavior that results in injury to a company and a consumer, even if the harm is precipitated by the criminality of a third party and "that a company's conduct was not *the most* proximate cause of an injury generally does not immunize liability from foreseeable harms."[158] The court's rejection of the former argument—that "unfair" behavior must be "marked by injustice, partiality, or deception"—was more creative. Pouncing on Wyndham's dictionary definition, the court issued a sharp rebuke of Wyndham's cybersecurity practices:

> *A company does not act equitably when it publishes a privacy policy to attract customers who are concerned about data privacy, fails to make good on that promise by investing inadequate resources in cybersecurity, exposes its unsuspecting customers to substantial financial injury, and retains the profits of their business.*[159]

Effectively folding the "deceptiveness" prong of Section 5 into its unfairness analysis, the court acknowledged that its rebuke "encompasses some facts relevant to the FTC's deceptive practices claim," but argued that "facts relevant to unfairness

155. *See Wydham II*, 799 F.3d at 244–45.

156. *Wyndham Opening App. Brief*, *supra* note 154, at 20–21.

157. *Id.* at 21.

158. *See Wyndham II*, 799 F.3d at 246. In reaching this conclusion, the Court cited the Second Restatement of Torts: "If the likelihood that a third person may act in a particular manner is the hazard or one of the hazards which makes the actor negligent, such an act[,] whether innocent, negligent, intentionally tortious, or criminal[,] does not prevent the actor from being liable for harm caused thereby." RESTATEMENT (SECOND) OF TORTS § 449 (AM. LAW INST. 1965); *see also* Westfarm Assocs. Ltd. P'ship v. Washington Suburban Sanitary Comm'n, 66 F.3d 669, 688 (4th Cir. 1995) (citing Scott v. Watson, 359 A.2d 548, 556 (Md. 1976)) ("Proximate cause may be found even where the conduct of the third party is . . . criminal, so long as the conduct was facilitated by the first party and reasonably foreseeable, and some ultimate harm was reasonably foreseeable.").

159. *Wyndham II*, 799 F.3d at 245.

and deception claims frequently overlap."[160] Somewhat surprisingly, and perhaps importantly, for future cases, the court collapsed Section 5's two prongs: "We cannot completely disentangle the two theories here."[161]

Third, the court rejected Wyndham's contention that "cybersecurity is no different in kind from physical security," and that endorsement of the FTC's present tactics vis-à-vis cybersecurity would give the Commission "authority to regulate the locks on hotel room doors," to "require every store in the land to post an armed guard at the door,"[162] or to sue supermarkets that are "sloppy about sweeping up banana peels."[163] After dismissing Wyndham's argument as "alarmist," the court concluded that, in any event, given the number of people implicated by the cyber attacks, Wyndham's were empty comparisons: "[this argument] invites 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 [Section 5]."[164]

Having concluded that Wyndham's conduct fell within the plain meaning of "unfair," the court then confronted Wyndham's contention that Congress' passage of the FCRA, COPPA, and the GLBA has reshaped Section 5's meaning to exclude cybersecurity.[165] In its brief, Wyndham argued that in each of these statutes Congress granted the FTC authority to regulate cybersecurity in specific types of situations, and "[t]hese tailored grants of substantive authority to the FTC in the cybersecurity field would be inexplicable if the Commission already had general

160. *Id.* (citing Am. Fin. Servs. Ass'n v. F.T.C., 767 F.2d 957, 980 n.27 (D.C. Cir. 1985)) ("The FTC has determined that . . . making unsubstantiated advertising claims may be both an unfair and a deceptive practice.").

161. *Id.* at 245. The Court seemed aware of the importance of this declaration, and devoted one of the longest footnotes in the opinion to defend its merger of the deception and unfairness analyses. *See id.* at 245 n.4 (citing Int'l Harvester Co., 104 F.T.C. 949, 1060 (1984)) ("[U]nfairness is the set of general principles of which deception is a particularly well-established and streamlined subset."); *In re* Figgie Int'l, 107 F.T.C. 313, 373 n.5 (1986) ("[U]nfair practices are not always deceptive but deceptive practices are always unfair."). Additionally, the Court qouted FTC staff member J. Howard Beales' statement on unfairness authority. *Wyndham II*, 799 F.3d at 245 n.4 ("Although, in the past, they have sometimes been viewed as mutually exclusive legal theories, Commission precedent incorporated in the statutory codification makes clear that deception is properly viewed as a subset of unfairness." (quoting Beales, *supra* note 12)); *see also* Neil W. Averitt, *The Meaning of "Unfair Acts or Practices" in Section 5 of the Federal Trade Commission Act*, 70 GEO. L.J. 225, 265 (1981) ("Although deception is generally regarded as a separate aspect of section 5, in its underlying rationale it is really just one specific form of unfair consumer practice.").

162. *Wyndham Opening App. Brief*, *supra* note 154, at 22–23.

163. *Wyndham II*, 799 F.3d at 246; *see also* Appellant's Reply Brief at 6, F.T.C. v. Wyndham Worldwide Corp., 799 F.3d 236 (3d Cir. 2015) (No. 14-3514), 2014 WL 7036128 [hereinafter *Wyndham Reply Brief*].

164. *Wyndham II*, 799 F.3d at 247.

165. *Id.* For a brief explanation of the FCRA, COPPA, and the GLBA, see *supra* notes 69–71 and accompanying text.

substantive authority over this field [in Section 5]."[166] The court countered that, in each of these statutes, Congress granted the Commission authorities above and beyond those emanating from Section 5: specifically, the FCRA required, rather than authorized, the FTC to issue regulations concerning cybersecurity and expanded the scope of the FTC's cybersecurity authority;[167] the GLBA similarly required the FTC to issue regulations and "relieves some of the burdensome [Section 5] requirements for declaring acts unfair";[168] and the Children's Online Privacy Protection Act required the FTC to issue regulations "and empowered it to do so under the procedures of the Administrative Procedure Act, rather than the more burdensome Magnuson-Moss procedures under which the FTC must usually issue regulations."[169] Because each of these statutes goes a little farther than Section 5, none of them would have been "inexplicable" if the FTC already had authority to regulate cybersecurity through Section 5.[170]

Finally, the court rejected Wyndham's contention that the FTC's interpretation of Section 5 was "inconsistent with its repeated efforts to obtain from Congress the very authority it purports to wield here."[171] Citing the testimony of various FTC officials in Congressional hearings, as well as the FTC's 2000 Report to Congress recommending cybersecurity legislation, Wyndham argued that "[f]or over a decade, the FTC has lobbied in favor of legislation that would establish substantive federal cybersecurity standards for American business, and give the FTC the

166. *Wyndham Opening App. Brief*, *supra* note 154, at 25. In support for the proposition that Congress' grant of specific regulatory authority suggests that the agency does not have a more general regulatory authority over the same conduct, Wyndham cited several Supreme Court cases. For example, see FDA v. Brown & Williamson Tobacco Corp., 529 U.S. 120, 143 (2000) ("The classic judicial task of reconciling many laws enacted over time, and getting them to make sense in combination, necessarily assumes that the implications of a statute may be altered by the implications of a later statute. This is particularly so where the scope of the earlier statute but the subsequent statutes more specifically address the topic at hand."); United States v. Estate of Romani, 523 U.S. 517, 530–31 (1998) ("[A] specific policy embodied in a later federal statute should control our construction of the [earlier] statute, even though it ha[s] not been expressly amended."); West Va. Univ. Hosps., Inc. v. Casey, 499 U.S. 83, 101 (1991) ("[I]t is our role to make sense rather than nonsense out of the *corpus juris*.").

167. *Wyndham II*, 799 F.3d at 248 (citing 15 U.S.C. § 1681w (2012)) ("The Federal Trade Commission . . . *shall* issue final regulations"); 15 U.S.C. § 1681m(e)(1)(B) ("The [FTC and other agencies] *shall* jointly . . . prescribe regulations requiring each financial institution . . . .").

168. *See Wyndham II*, 799 F.3d at 248 (citing 15 U.S.C. § 6801(b) (2011)) ("[The FTC] shall establish appropriate standards . . . to protect against unauthorized access to or use of . . . records . . . which could result in substantial harm *or inconvenience to any customer*."). As evidence of how the GLBA unburdens the FTC of Section 5's requirements, the Court cited § 6801(b) of the GLBA, "[The FTC] shall establish appropriate standards . . . to protect against unauthorized access to or use of . . . records . . . which could result in substantial harm *or inconvenience to any customer*." 15 U.S.C. §6801(b) (2011) (emphasis added).

169. *Id.* at 248 (internal citations omitted).

170. *Id.* at 247.

171. *Id.* at 248 (quoting *Wyndham Opening App. Brief*, *supra* note 154, at 28).

authority to enforce those standards."[172] Identifying FCC testimony to the same effect, the court concluded that the FTC's requests for codification of the broad "fair information practice principles" did not amount to an admission that it did not have authority to prosecute cybersecurity cases under Section 5's "unfairness" prong.[173]

2. Fair Notice

With respect to the second question certified for review, whether Wyndham had fair notice it could be targeted by the FTC for its cybersecurity practices, the court first delineated the various standards for fair notice, depending on the type of case.[174] Critically, the court had to determine whether there was an FTC rule or adjudication regarding the application of Section 5's unfairness prong to cybersecurity, in which case Wyndham was entitled to "ascertainable certainty" of the FTC's interpretation of what specific cybersecurity practices are required by Section 5,[175] or whether, in the absence of an applicable regulation or adjudication, Wyndham was only entitled to fair notice that its conduct could fall within the meaning of the statute.[176] In concluding there was no applicable regulation or

172. *Wyndham Opening App. Brief*, *supra* note 154, at 28; *see* 2000 Report, *supra* note 62, at 34. *See generally Consumer Data Protection: Hearing Before the Subcomm. on Commerce, Mfg. & Trade of the H. Comm. on Energy & Commerce*, 112th Cong. (2011) (statement of Edith Ramirez, Comm'r, FTC); *Data Theft Issues: Hearing Before the Subcomm. on Commerce, Mfg. & Trade of the H. Comm. on Energy & Commerce*, 112th Cong. (2011) (statement of David C. Vladeck, Director, FTC Bureau of Consumer Protection).

173. *Wyndham II*, 799 F.3d at 248–249.

174. *Id.* at 249–55. The critical issue with respect to "fair notice" in this context was whether a defendant had fair notice of a court's, or an agency's, interpretation of a particular statute. The court differentiated between fair notice standards in at least five different types of cases: (1) criminal cases, (2) civil cases involving statutes governing economic behavior, (3) cases where an agency is administering a statute without conferring new rights or obligations, (4) cases where an agency issues regulations to fill in a statutory gap, and (5) cases where an agency is interpreting its own regulation. *Id.*

175. *Id.* at 253–54.

176. *Id.* at 253. The court explained that the reason for the difference between fair notice standards for cases where the agency is interpreting a statute (in promulgating regulations or adjudicating a case) and fair notice standards where the agency is merely administering a statute:

> A higher standard of fair notice applies in the second and third contexts than in the typical civil statutory interpretation case because agencies engage in interpretation differently than courts. In resolving ambiguity in statutes or regulations, courts generally adopt the best or most reasonable interpretation. But, as the agency is often free to adopt any reasonable construction, it may impose higher legal obligations than required by the best interpretation.
>
> Furthermore, courts generally resolve statutory ambiguity by applying traditional methods of construction. Private parties can reliably predict the court's interpretation by applying the same methods. In contrast, an agency may also rely on technical expertise and political values. It is harder to predict how an agency will construe a statute or regulation at some unspecified point in the future, particularly when that interpretation will depend on the "political views of the President in office at [that] time."

adjudication preceding Wyndham's alleged violation of Section 5, the court turned Wyndham's own argument on its head, citing seven different places, in court filings and oral argument, where Wyndham had asserted that the FTC's motion to dismiss order in *LabMD* (the potential prior adjudication on which Wyndham focused its argument) did *not* merit deference by the court.[177] Because Wyndham was, in other words, "asking the federal courts to interpret [Section 5] in the first instance to decide whether it prohibits the alleged conduct here," Wyndham was not entitled to "ascertainable certainty" about the FTC's interpretation of Section 5, only fair notice of whether its conduct may have been deemed unfair under Section 5 (as determined by a court).[178]

Having dispatched Wyndham's "ascertainable certainty" arguments, the court turned to what fair notice standard applied, concluding that, because the case involved a civil statute governing economic activity, the relevant inquiry was whether the unfairness prong of Section 5 was "so vague as to be 'no rule or standard at all.'"[179] In determining that the statute was not in fact "so vague," the court noted that Section 5 "asks whether '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'"[180]:

> *While far from precise, this standard informs parties that the relevant inquiry here is a cost-benefit analysis that considers a number of relevant factors, including the probability and expected size of reasonably unavoidable harms to consumers given a certain level of cybersecurity and the costs to consumers that would arise from investment in stronger cybersecurity.*[181]

Id. at 251–52.

177. *Id.* at 252–54.

178. *Id.* at 253, 255 ("For now, however, it is enough to say that we accept Wyndham's forceful contention that we are interpreting the FTC Act (as the District Court did). As a necessary consequence, Wyndham is only entitled to notice of the meaning of the statute and not to the agency's interpretation of the statute.").

179. *Id.* at 255 (citations omitted) ("Wyndham is entitled to a relatively low level of statutory notice for several reasons. [Section 5] does not implicate any constitutional rights here. It is a civil rather than criminal statute. And statutes regulating economic activity receive a 'less strict' test because their 'subject matter is often more narrow, and because businesses, which face economic demands to plan behavior carefully, can be expected to consult relevant legislation in advance of action.' In this context, the relevant legal rule is not 'so vague as to be "no rule or standard at all."'").

180. *Wyndham II*, 799 F.3d at 255.

181. *Id.* at 255–56 (citations omitted) ("We acknowledge there will be borderline cases where it is unclear if a particular company's conduct falls below the requisite legal threshold. But under a due process analysis a company is not entitled to such precision as would eliminate all close calls. Fair notice is satisfied here as long as

Treating Wyndham's as an "as-applied" challenge, the court noted that the FTC did not merely allege that Wyndham had used weak firewalls, IP address restrictions, encryption software, and passwords, but, instead, "that Wyndham failed to use *any* firewall at critical network points, did not restrict specific IP addresses *at all*, did not use *any* encryption for certain customer files, and did not require some users to change their default or factory-setting passwords *at all*."[182] The court also leaned on the fact that Wyndham was hacked "not one or two, but three, times"— "At least after the second attack," the court said, "it should have been painfully clear to Wyndham that a court *could* find its conduct failed the cost-benefit analysis."[183]

Additionally, the court highlighted that the FTC had filed a number of complaints and issued a number of consent decrees defining the contours of what constitutes acceptable data security practices, in addition to issuing a data security guidebook in 2007 which included advice that would have prevented or mitigated the damage from Wyndham's failures.[184]

Finally, the court rejected, on two grounds, Wyndham's argument that the FTC's complaint was too vague because it failed to delineate which specific cybersecurity practices triggered the Section 5 violation, instead lumping together a number of practices that, taken together, fail the cost-benefit analysis.[185] First, the court concluded that "even if the complaints do not specify which allegations . . . form the necessary and sufficient conditions of the alleged violation, they can still help companies apprehend the possibility of liability under the statute."[186] Second, the court compared the FTC's complaint against Wyndham to an earlier, analogous case against CardSystems Solutions in 2006: "Wyndham cannot argue that the complaints fail to give notice of the necessary and sufficient conditions of an alleged

the company can reasonably foresee that a court could construe its conduct as falling within the meaning of the statute.").

182. *Id.* at 256 (citations omitted).

183. *Id.* Because the relevant issue is whether Wyndham was on fair notice that its actions could fall within the ambit of Section 5, the court left unanswered the fact question of whether Wyndham's practices were actually unfair under Section 5. *Id.* ("We leave for another day whether Wyndham's alleged cybersecurity practices do in fact fail, an issue the parties did not brief.").

184. *Id.* at 257 ("That the FTC commissioners . . . believe that alleged cybersecurity practices fail the cost-benefit analysis of [Section 5] certainly helps companies with similar practices apprehend the possibility that their cybersecurity could fail as well."); Gerald J. Ferguson & Alan L. Friel, *Challenging FTC Regulation of Cyber-security After* FTC v. Wyndham, DATA PRIVACY MONITOR BLOG, (Nov. 4, 2016), http://www.dataprivacymonitor.com/cybersecurity/challenging-ftc-regulation-of-cyber-security-after-ftc-v-wyndham (quoting *Wyndham II*, 799 F.3d at 257 n.22) ("The consent orders, which admit no liability and which focus on prospective requirements on the defendant, were of little use to it in trying to understand the specific requirements imposed by § 45(a).").

185. *Wyndham II*, 799 F.3d at 258.

186. *Id.*

§ 45(a) violation when all of the allegations in at least one of the relevant four or five complaints have close corollaries here."[187]

D. Wyndham *Settles*

Although Wyndham vowed to continue fighting after the Third Circuit's ruling, a little more than three months later, the company settled the case.[188] "This settlement marks the end of a significant case in the FTC's efforts to protect consumers from the harm caused by unreasonable data security," said FTC Chairwoman Edith Ramirez.[189] "Not only will it provide important protection to consumers, but the court rulings in the case have affirmed the vital role the FTC plays in this important area."[190]

The settlement, outlined in a stipulated order from the district court, did not require Wyndham to pay any monetary penalties, but the terms nevertheless illustrate the long-term burden faced by a company that loses a cybersecurity case brought by the Commission.[191] The company is required to establish a comprehensive information security program designed to protect cardholder data, including payment card numbers, names and expiration dates.[192] In addition, the company is required to conduct annual information security audits and maintain safeguards in connections to its franchisees' servers which conform to the Payment Card Industry Data Security Standards.[193] The settlement also requires Wyndham's

187. *Id.*

188. Press Release, Jessica Rich, Dir., Fed. Trade Comm'n, Bureau of Consumer Prot., Wyndham Settles FTC Charges It Unfairly Placed Consumers' Payment Card Information At Risk (Dec. 9, 2015), https://www.ftc.gov/news-events/press-releases/2015/12/wyndham-settles-ftc-charges-it-unfairly-placed-consumers-payment [hereinafter Rich, Press Release]; *see also* Sophia Pearson, *Wyndham Must Face Hacker Suit as Court Upholds FTC Power*, BLOOMBERG (Aug. 24, 2015), http://www.bloomberg.com/news/articles/2015-08-24/wyndham-must-face-ftc-suit-for-failing-to-stop-russian-hackers ("Once the discovery process resumes, we believe the facts will show the FTC's allegations are unfounded . . . Safeguarding personal information remains a top priority for our company and, with the dramatic increase in the number and severity of cyberattacks on both public and private institutions, we believe consumers will be best served by the government and businesses working together collaboratively rather than as adversaries.").

189. Rich, Press Release, *supra* note 188.

190. *Id.*

191. *See* Stipulated Order for Injunction at 4–14, Fed. Trade Comm'n. v. Wyndham Worldwide Corp, et al., 10 F. Supp. 3d 602 (D. N.J. Dec. 11, 2015) (No. 2:13-CV-01887-ES-JAD) [hereinafter *Wyndham's Stipulated Order*].

192. *Id.*; *see also* Daren Orzechowski & Thomas Cockriel, *FTC and Wyndham Settle Suit Regarding Wyndham's Alleged Cybersecurity Failures*, WHITE & CASE TECH. NEWS FLASH (Jan. 19, 2016), http://www.whitecase.com/publications/article/ftc-and-wyndham-settle-suit-regarding-wyndhams-alleged-cybersecurity-failures.

193. *See PCI Security*, PCI SEC. STANDARDS COUNCIL, https://www.pcisecuritystandards.org/pci_security (last visited Feb. 17, 2017). The PCI Security Standards Council was founded in 2006 by American Express, Discover, JCB International, MasterCard and Visa Inc., for the promotion of security standards in the payment

audit to: (1) certify the "untrusted" status of certain franchisee networks, to prevent future hackers from using the same methods; (2) implement a formal risk assessment process for analyzing the possible data security risks faced by the company; and (3) certify that the auditor is "qualified, independent and free from conflicts of interest."[194]

In the event Wyndham suffers another data breach affecting more than 10,000 payment card numbers, the company must obtain an assessment of the breach and provide that assessment to the FTC within 10 days.[195] Wyndham must submit to the FTC a compliance report describing the activities the company has taken to comply with the stipulated order and, during the 10 years after filing, submit notice of any change in the structure of Wyndham or any Wyndham subsidiary that may affect compliance with the obligations under the settlement.[196] The settlement provides that if Wyndham successfully obtains the necessary compliance certifications, it will be deemed in compliance with the comprehensive information security program provision of the order.[197] Wyndham's obligations under the settlement are in place for 20 years.[198]

E. LabMD *at the Eleventh Circuit?*

Although the Third Circuit's endorsement of the FTC's use of the unfairness doctrine in *Wyndham* was significant, it is unlikely the case will be the last word on the issue. Indeed, it looks increasingly like *LabMD* will be the next chance federal courts have to sound off on the FTC's cybersecurity tactics: in July 2016, the Commission voted to overturn the ruling of an administrative law judge ("ALJ") granting LabMD's motion to have the FTC's action dismissed—the ALJ issued the ruling on the grounds that the FTC had failed to show LabMD's security practices caused or were likely to cause substantial harm[199]—ripening the case for review before the Eleventh Circuit.[200]

card industry. *Id.* The organization lists its two priorities as, "[h]elping merchants and financial institutions understand and implement standards for security policies, technologies and ongoing processes that protect their payment systems from breaches and theft of cardholder data," and "[h]elping vendors understand and implement standards for creating secure payment solutions." *Id.*

194. Rich, Press Release, *supra* note 188.

195. *Id.*

196. *Wyndham's Stipulated Order*, *supra* note 191, at 12.

197. Rich, Press Release, *supra* note 188.

198. *Id.*

199. *See* Press Release, Fed. Trade Comm'n, Administrative Law Judge Dismisses FTC Data Security Complaint Against Medical Testing Laboratory LabMD, Inc. (Nov. 19, 2015), https://www.ftc.gov/news-events/press-releases/2015/11/administrative-law-judge-dismisses-ftc-data-security-complaint; Initial Decision, *In re* LabMD Inc., No. 9357, 2015 WL 7575033, at *3 (F.T.C. Nov. 13, 2015) *vacated* by Public Opinion of the

Critical to the ALJ's ruling, issued in November of 2015, was the suspect evidence of harm offered by Tiversa, the cyber intelligence company that first brought the alleged security breach to LabMD's, and then the FTC's, attention.[201] The judge noted that the FTC's decision to launch an investigation and prosecute LabMD rested on evidence from Tiversa that the 1718 file had been compromised, and also highlighted the Oversight Committee's report on Tiversa, in addition to the testimony of a former Tiversa employee that Tiversa had manipulated evidence to try and get LabMD's business, and then, when LabMD rejected their offer, reported the company to the FTC in retaliation.[202] Reviewing the expert testimony from both sides, the judge concluded that the FTC had failed to show that consumers had suffered, or were likely to suffer, substantial injury as a result of LabMD's alleged security failures.[203]

The following July, a full panel of commissioners voted to overturn the dismissal, finding that the Commission did not need to show the kind of tangible injuries required by the ALJ.[204] In a 37-page opinion, FTC Chairwoman Edith Ramirez wrote: "The ALJ held that 'privacy harms, allegedly arising from an unauthorized exposure of sensitive medical information . . . unaccompanied by any tangible injury such as monetary harm or health and safety risks, [do] not constitute "substantial injury" within the meaning of Section 5(n).' We disagree."[205] Central to the Commission's case was the fact that Tiversa had obtained the file; Ramirez explained:

> *It is undisputed that the 1718 file contained names, dates of birth, social security numbers, insurance company names, policy numbers, and codes for laboratory tests performed, including tests for HIV, herpes, prostate cancer, and testosterone levels. We also know that the file was downloaded by at least one unauthorized third-party – Tiversa – and then shared with an academic researcher.*[206]

Commission, *In re* LabMd, Inc., No. 9357, 2016 WL 4128215 (F.T.C. July 28, 2016) [hereinafter *LabMD Dismissal*]. For discussion of the substantial harm factor, see *supra* Section II.B.

200. Public Opinion of the Commission at 1, *In re* LabMd, Inc., No. 9357, 2016 WL 4128215 (F.T.C. July 28, 2016) [hereinafter *Wyndham, Opinion of Commission*].

201. *See LabMD Dismissal*, *supra* note 199, at 6–7.

202. *See id.* at 6–11.

203. *Id.* at 69 ("For all the foregoing reasons, the evidence fails to prove that consumers whose information was contained in the 1718 File have suffered, or are likely to suffer, substantial injury as a result of the exposure of the 1718 File. Therefore, the exposure of the 1718 File does not support Complaint Counsel's assertion that Respondent's data security practices are likely to cause substantial consumer harm.").

204. *Wyndham Opinion of Commission*, *supra* note 200, at 17.

205. *Id.* (alteration in original) (citations omitted).

206. *Id.* (citations omitted).

Although the FTC has not, to date, shown that the leak of the 1718 file resulted in identity theft, the Commission noted that this was irrelevant: what matters is whether LabMD's practices were likely to result in injury.[207] Moreover, the likely injury need not be monetary.[208] According to Ramirez, the mere possibility of disclosure of medical information and subsequent "embarrassment" is enough to bring a Section 5 claim:

> *We conclude that the disclosure of sensitive health or medical information causes additional harms that are neither economic nor physical in nature but are nonetheless real and substantial and thus cognizable under Section 5(n). For instance, Complaint Counsel's expert, Rick Kam, testified that disclosure of the mere fact that medical tests were performed irreparably breached consumers' privacy, which can involve "embarrassment or other negative outcomes, including reputational harm.*[209]

Obviously, this is different from the theft of payment card numbers by Russian hackers and estimated millions of dollars in fraud loss alleged in *Wyndham*.[210]

In late September 2016, a request for the Commission to stay the effective date of its action against LabMD pending planned appeals to the Eleventh Circuit was denied,[211] but a subsequent stay request to the Eleventh Circuit was granted in November.[212]

---

207. *Id.* ("Complaint Counsel introduced evidence of a range of harms that can and often do result from the unauthorized disclosure of sensitive personal information of the types contained in the 1718 file.").

208. *See id.*

209. *Id.*

210. Also central to Ramirez's argument was the notion that the FTC treats medical information differently. Opinion of Commission, *supra* note 201, at 18 ("Indeed, the Commission has long recognized that the unauthorized release of sensitive medical information harms consumers." (first citing F.T.C. v. Eli Lilly & Co., 133 F.T.C. 763, 767–68 (2002); then citing Complaint at 4, *In re* GMR Transcription Services, Inc., 2014 WL 4252393 (Aug. 14, 2014))). Ramirez also noted the "broad recognition in federal and state law of the inherent harm in the disclosure of sensitive health and medical information," *Id.* at 18–19 (first citing Health Insurance Portability & Accountability Act, 42 U.S.C. §§ 1320 (1996); then citing Health Information Technology for Economic and Clinical Health Act, 42 U.S.C. §§ 300jj (2009)). There are heightened protections for medical information in federal case law and in tort principles. *See, e.g.*, *id.* at 19 (first citing Maracich v. Spears, 133 S. Ct. 2191, 2202 (2013); then citing Harris v. Thigpen, 941 F.2d 1495, 1513–14 (11th Cir. 1991)); RESTATEMENT (SECOND) OF TORTS § 652D, cmt. b (AM. LAW INST. 1977) ("As explained by the Restatement of Torts, when 'intimate details of [one's] life are spread before the public gaze in a manner highly offensive to the ordinary reasonable man, there is an actionable invasion of his privacy, unless the matter is one of legitimate public interest.'").

211. LabMD, Inc. v. F.T.C., No. 16–16270–D, 2016 WL 8116800, at *2 (11th Cir. Nov. 10, 2016) (reviewing LabMd's requested stay, following the FTC Final Order that denied the stay); *see also* Jimmy H. Koo, *LabMD Wants Stay of Landmark FTC Data Security Ruling*, BLOOMBERG BNA (Aug. 31, 2016), http://www.bna.com/labmd-wants-stay-n73014447214/?utm_campaign=LEGAL_NWSLTR_Privacy+%26+Data+Security+Law+Update_090716&utm_medium=email&utm_source=Eloqua&elqTrackId=ece70288cdce4

In deciding whether to grant the stay, the Eleventh Circuit focused primarily on whether LabMD was likely to prevail on the merits on appeal, and specifically whether LabMD's practice, as the FTC alleges, "causes or is likely to cause substantial injury to consumers" under Section 5.[213] The court reasoned that "[t]he FTC's ruling did not point to any tangible harm to any consumer, because there is no evidence that any consumer suffered a harm such as identity theft or physical harm," noting that the harms alleged by the FTC were pinned solely on the exposure of the 1718 file.[214] The Court then gave two reasons why the FTC's interpretation of Section 5 might be unreasonable. First, the Court argued that it "is not clear that a reasonable interpretation of [Section 5] includes intangible harms like those that the FTC found in this case."[215] Second, the Court argued that the FTC's holding that "likely to cause" does not mean "probable," but instead means "significant risk," is not a reasonable interpretation—"[W]e do not read the word 'likely' to include something that has a low likelihood," the Court reasoned. "We do not believe an interpretation that does this is reasonable."[216]

The Court also issued a stark summary of the financial harm LabMD suffered as a result of the FTC investigation and ongoing litigation, and the likely irreparable harm to LabMD if the stay were not granted, the summary of which is worth quoting in full:

> *LabMD is no longer an operational business. It has no personnel and no revenue. It now has less than $5,000 cash on hand. It reported a loss of $310,243 last fiscal year, and has a pending $1 million judgment against it*

f0aa58ff456d2f60732&elq=650ea4e7a16247208ff4b5d2805031f0&elqaid=6271&elqat=1&elqCampaignId=3738 (last visited Feb. 14, 2016).

212. *LabMD, Inc.*, 2016 WL 8116800, at *1.

213. *Id.* at *2 (referencing Section 5 of FTC's authority). The Court identified four factors that constitute the "traditional standard" for considering a stay:

> (1) whether the stay applicant has made a strong showing that he is likely to succeed on the merits; (2) whether the applicant will be irreparably injured absent a stay; (3) whether issuance of the stay will substantially injure the other parties interested in the proceeding; and (4) where the public interest lies.

Id. (quoting Nken v. Holder, 556 U.S. 418, 425–26, 434 (2009)). The Court went on to specify that, "'[t]he first two factors . . . are the most critical.'" *Id.*

214. *Id.* at *3 ("Instead, the FTC found actual harm here due to the sole fact of the 1718 file's unauthorized disclosure. The FTC also found that consumers suffered a 'privacy harm' that may have affected their reputations or emotions, which therefore constituted a substantial injury. Alternatively, the FTC found that the unauthorized exposure of the 1718 file was likely to cause substantial injury.").

215. *Id.* ("LabMD points out that what the FTC here found to be harm is 'not even "intangible,"' as a true data breach of personal information to the public might be, 'but rather is purely conceptual' because this harm is only speculative. LabMD has thus made a strong showing that the FTC's factual findings and legal interpretations may not be reasonable.").

216. *Id.* at *9.

> *on account of its early termination of its lease. LabMD cannot even afford legal representation, and is relying on pro bono services for this appeal.*
>
> *Ordinary compliance costs are typically insufficient to render harm irreparable. But given LabMD's bleak outlook, the costs of compliance pending appeal would constitute an irreparable harm.*[217]

The Court's order, and perhaps even sympathy for LabMD's plight, is clearly the most positive development for the company to date. It is also the strongest evidence that the FTC's unfairness-focused methods of policing cybersecurity could be in jeopardy. If, as seems increasingly likely, the case gets a *Wyndham*-like hearing before that court, *LabMD* may, for several reasons, be a better test of the Commission's application of its unfairness authority to cybersecurity.[218]

For one, the case against LabMD does not include allegations of deceptiveness, precluding the Eleventh Circuit from following the Third Circuit and folding the deceptiveness and unfairness prongs into a single argument.[219] As discussed above, the fact that Wyndham "publishe[d] a privacy policy to attract customers who [we]re concerned about data privacy," and "fail[ed] to make good on that promise by investing inadequate resources in cybersecurity," was central to the Third Circuit's conclusion that Wyndham had failed to act "equitably."[220]

Second, whereas Wyndham suffered three different security breaches over a two year period, "failed to remedy known security vulnerabilities," and "failed to follow proper incident response procedures,"[221] the FTC's case against LabMD centers on one security breach caused by a deficiency, the presence of Limewire on an employee's computer, which LabMD remedied immediately upon receiving notice.[222] As discussed above, the Third Circuit's conclusion in *Wyndham* that the hotelier was on fair notice depended in part on the fact that Wyndham had suffered multiple breaches.[223] Although the FTC's complaint against LabMD mentions evidence of a second breach—the "day sheets" discovered by the Sacramento Police

217. *Id.* at *4.

218. *See* Craig A. Newman, *The Long and Wyndham Road: A Settlement in* Wyndham *and Curve Ball in LabMD Signals Storm Warnings for the FTC's 2016 Data Security Initiatives*, BLOOMBERG BNA (Jan. 4, 2016), http://www.bna.com/long-wyndham-road-n57982065672. For a straightforward critique of the Third Circuit's decision in *Wyndham*, see Christin S. McMeley, Wyndham*: Did The Third Circuit Get It Wrong?*, BLOOMBERG BNA (Sep. 14, 2015), http://www.bna.com/wyndham-third-circuit-n17179935994.

219. *Compare Wyndham Complaint*, *supra* note 2, at 18–19, *with LabMD Complaint*, *supra* note 3, at 5.

220. F.T.C. v. Wyndham Worldwide Corp. (*Wyndham II*), 799 F.3d 236, 245 (3d Cir. 2015); *see supra* notes 135–137.

221. *Wyndham Complaint*, *supra* note 2, at 10–12.

222. *LabMD Complaint*, *supra* note 3, at 5 ("Respondent had no business need for Limewire and removed it from the billing computer in May 2008, after receiving notice.").

223. *Wyndham II*, 799 F.3d. at 256.

Department, which contained information post-dating the 1718 file—the FTC does not allege that LabMD was aware of any such breach.[224]

Third, as discussed above in this section, the *LabMD* case does not include allegations of actual fraud loss, as in *Wyndham*.[225] Granting that the Commission only has to show a likelihood of substantial injury to consumers, the *LabMD* case would present a novel question for the Eleventh Circuit, not taken up in *Wyndham*: whether the disclosure of medical information alone, as a result of a cyber breach, constitutes a substantial injury for Section 5 purposes. As discussed above, the "substantial financial injury" suffered by Wyndham customers was central to the *Wyndham* court's notion of unfairness.[226]

Finally, aside from the fewer number of known breaches, and immediate remediation, LabMD, a smaller corporation which has (allegedly) been forced to close its doors because of the FTC's investigation, is generally a more sympathetic defendant than Wyndham, as is evidenced by the recent Eleventh Circuit order granting the company a stay. If the broad question in *Wyndham* seemed to be whether a large company could be careless with customers' data while riding off into the sunset with their money, the more salient question in LabMD may be whether the FTC can shut down any business unlucky enough to be targeted by hackers, even where the business immediately redresses its security deficiencies.

IV. THE FTC AND PRIVACY BY DESIGN

The Third Circuit's decision in *Wyndham* reaffirms that when a company has been careless about its cybersecurity practices and deceived consumers into thinking they're safe, its conduct may be deemed "unfair." But what if a company hasn't been deceptive? Can the FTC enforce a set of cybersecurity standards purely on the basis of what it deems "fair" under Section 5? Would such a broad, "unfairness-only" regulatory mandate not transform the FTC into the *de facto*, if not *de jure*, national cybersecurity agency and supplant congressional authority? These questions remain unresolved.

What *is* clear, for the time being, is that the FTC has continually broadening—and, now, judicially sanctioned—authority to police cybersecurity under the unfairness prong (including deceptiveness as a factor). To what degree the Commission will be emboldened by the Third Circuit's decision remains to be seen, but there's no reason to believe that, as cybersecurity threats continue to grow, the FTC won't continue stepping up policing efforts under the unfairness prong, as it has for years. Accordingly, it will be increasingly important for businesses of all sizes to comb the FTC's complaints, consent decrees, guidebooks, congressional reports,

224. *See LabMD Complaint*, *supra* note 3, at 2, 4–5.

225. *Wyndham Complaint*, *supra* note 2, at 2.

226. *See supra* note 160–161 and accompanying text.

and policy statements to discern exactly what the Commission has in mind regarding data security and privacy. Central to understanding the FTC's vision, this paper argues, is understanding "Privacy by Design."

A. What is Privacy by Design?

Credit for the concept of "Privacy by Design" (also referred to as "PbD") goes to Dr. Ann Cavoukian, formerly the Information and Privacy Commissioner of Ontario, Canada, who first introduced the "foundational principles" of PbD in the mid-1990s.[227] According to Cavoukian, Privacy by Design "advances the view that the future of privacy cannot be assured solely by compliance with regulatory frameworks; rather, privacy assurance must ideally become an organization's default mode of operation."[228] Elsewhere, Cavoukian has explained that PbD "represents a significant shift from traditional approaches to protecting privacy, which focus on setting out minimum standards for information management practices, and providing remedies for privacy breaches, after-the-fact."[229] Likewise, Alexander Dix, Berlin Commissioner for Data Protection and Freedom of Information, has described older privacy approaches as being akin to "locking the stable door after the horse has bolted."[230]

The seven principles of PbD which, according to Cavoukian's framework, aim to make privacy a priority rather than an afterthought, are:

1. Proactive not Reactive; Preventative not Remedial: "The Privacy by Design (PbD) approach is characterized by proactive rather than reactive measures. It anticipates and prevents privacy invasive events before they happen."
2. Privacy as the Default Setting: "Privacy by Design seeks to deliver the maximum degree of privacy by ensuring that personal data are automatically protected in any given IT system or business practice."
3. Privacy Embedded into Design Privacy by Design: "Privacy by Design is embedded into the design and architecture of IT

227. In 2014, Cavoukian left her Commissioner post to become the executive director of the Privacy and Big Data Institute at Ryerson University in Ontario. *See* Ann Cavoukian, PRIVACY & BIG DATA INSTITUTE, RYERSON UNIV. (2017), http://www.ryerson.ca/pbdi/about/people/cavoukian.html (last visited Feb. 15, 2017). The FTC gives Cavoukian credit for the concept in its 2010 and 2012 reports. *See* 2010 Report, FED. TRADE COMM'N, *supra* note 66, at v, n.3; 2012 Report, FED. TRADE COMM'N, *supra* note 66, at 1, n.2.

228. Ann Cavoukian, *Privacy by Design*, INFORMATION & PRIVACY COMMISIONER (Jan. 2011), https://www.ipc.on.ca/wp-content/uploads/Resources/7foundationalprinciples.pdf.

229. Ann Cavoukian, 33rd International Conference of Data Protection and Privacy Commissioners, *Report on State of PbD*, at 3 (2011) [hereinafter Caoukian, *Report on State of PbD*].

230. *Id.*

systems and business practices. It is not bolted on as an add-on, after the fact."

4. Full Functionality: "Privacy by Design seeks to accommodate all legitimate interests and objectives in a positive-sum 'win-win' manner, not through a dated, zero-sum approach, where unnecessary trade-offs are made."
5. End-to-End Security: "Privacy by Design, having been embedded into the system prior to the first element of information being collected, extends securely throughout the entire lifecycle of the data involved — strong security measures are essential to privacy, from start to finish."
6. Visibility and Transparency: "Privacy by Design seeks to assure all stakeholders that whatever the business practice or technology involved, it is in fact, operating according to the stated promises and objectives, subject to independent verification."
7. Respect for User Privacy: "Above all, Privacy by Design requires architects and operators to keep the interests of the individual uppermost by offering such measures as strong privacy defaults, appropriate notice, and empowering user-friendly options."[231]

Cavoukian's PbD principles have become globally recognized standards.[232] The tipping point perhaps came in October 2010, at the 32nd International Conference of Data Protection and Privacy Commissioners (ICDPPC) in Jerusalem, when privacy regulators from all over the world passed the "Resolution on Privacy by Design," also known as the "Jerusalem Declaration," recognizing PbD as "an essential component of privacy protection" and resolving to promote Cavoukian's principles.[233]

The concept of PbD has proven to be both popular and malleable.[234] Microsoft, for example, explains on its website that "'Privacy by Design' has become a popular

231. *Id.* at 4.

232. *See, e.g.*, Sam Pfeifle, "*Privacy by Default*" *May Be Big Post-Regulation Issue*, IAPP, Sep. 30, 2013, https://iapp.org/news/ a/privacy-by-default-may-be-big-post-regulation-issue (last visited Apr. 10, 2016) ("At this point, 'Privacy by Design' is as close to privacy dogma as you're going to get. Regulatory bodies across the globe now provide this idea, developed by Ontario Information and Privacy Commissioner Ann Cavoukian, as guidance for all technology companies that hope to gather personal information.").

233. 32nd International Conference of Data Protection and Privacy Commissioners, *Resolution on Privacy by Design* (Oct. 27-29, 2010), https://icdppc.org/wp-content/uploads/2015/02/32-Conference-Israel-resolution-on-Privacy-by-Design.pdf [hereinafter "Jerusalem Declaration"].

234. *See* Kashmir Hill, *Why 'Privacy by Design' Is the New Corporate Hotness*, FORBES (Jul. 28, 2011), http://www.forbes.com/sites/kashmirhill/2011/07/28/why-privacy-by-design-is-the-new-corporate-hotness/#4388394777de.

term in the privacy community, but it means different things to different people,"[235] and lists six different "privacy principles" governing its use of consumer data.[236] Likewise, Article 23 of the European Union's General Data Protection Regulation (GDPR), a comprehensive privacy and data security law first proposed in 2012 and formally adopted in late 2015, requires that controllers of the data of EU citizens "implement mechanisms for ensuring that, by default, only those personal data are processed which are necessary for each specific purpose of the processing and are especially not collected or retained beyond the minimum necessary for those purposes."[237] Google, Twitter, and Mozilla have all drawn praise for implementing PbD-style policies, including most notably default encryption.[238]

Finally, several industry-wide and non-profit security initiatives in the private sector have also often sought to implement PbD-style privacy recommendations, including the PCI Data Security Standards for payment card data,[239] the SANS Institute's security policy templates,[240] and guidelines for the financial services industry provided by BITS, the technology policy division of the Financial Services Roundtable.[241]

B. The FTC and PbD

The FTC first rolled out PbD as an official policy in its 2010 privacy report, as one of three components of a "proposed framework" for data security, the other two

235. *See Our Commitment*, MICROSOFT, https://www.microsoft.com/en-us/twc/privacy/commitment.aspx [http://web.archive.org/web/20160503113053/https://www.microsoft.com/en-us/twc/privacy/commitment.aspx] (last visited May 3, 2016) ("At Microsoft, Privacy by Design describes not only how we build products but also how we operate our services and organize ourselves as an accountable technology leader."). Microsoft divides its privacy commitment into four areas: "Practices," "Policy Activity," "Research," and "Privacy Models." *Id.*

236. *Privacy at Microsoft*, MICROSOFT, https://privacy.microsoft.com/en-US [http://web.archive.org/web/20170131184655/https://privacy.microsoft.com/en-us/] (last visited Jan. 31, 2017).

237. Caoukian, *Report on State of PbD*, supra note 229, at 3.

238. *See* 2012 Report, FED. TRADE COMM'N, *supra* note 66, at 25–26 ("Google has cited certain security features in its products, including default SSL encryption for Gmail and security features in its Chrome browser. Similarly, Mozilla has noted that its cloud storage system encrypts user data using SSL communication. Likewise, Twitter has implemented encryption by default for users logged into its system."); *see also* Edith Ramirez, Commissioner, Fed. Trade Comm'n, Remarks at the Privacy by Design Conference: Privacy By Design and the New Privacy Framework of the U.S. Federal Trade Commission (June 13, 2012) (listing Google, Twitter, Mozilla, Apple's Safari internet browser, and Microsoft's X-Box as examples of privacy by design).

239. *See supra* note 193.

240. *Information Security Policy Templates*, SANS INSTITUTE, https://www.sans.org/security-resources/policies (last visited Feb. 15, 2017). The SANS Institute is a non-profit group established in 1989 as "a cooperative research and education organization," for studying and discussing information security. *See About*, SANS INSTITUTE, https://www.sans.org/about (last visited Feb. 15, 2017).

241. *See BITS Publications*, FIN. SERVS. ROUNDTABLE, at 1–2 http://fsroundtable.org/bits/publications#2 (last visited Feb. 15, 2017).

components being "simplified choice" and "greater transparency."[242] With respect to the PbD component, the 2010 Report identified four key "protections" that business should build into "their every day business practices"—data security, reasonable collection limits, sound retention practices, and data accuracy—as well as a fifth procedural principle requiring companies to "maintain comprehensive data management procedures throughout the life cycle of their products and services."[243] The report did not elaborate extensively on what types of procedures would be sufficient, but recommended "assigning personnel to oversee privacy issues from the earliest stages of research and development, training employees on privacy, and conducting privacy reviews of new products and services."[244] The report was the culmination of a year of "roundtables" conducted by the Commission with "academics, technologists, privacy experts, consumer advocates, representatives from industry, and regulators" about what a data security framework should look like.[245] After issuing its 2010 report, the FTC received more than 450 public comments from various stakeholders, and based on this feedback issued a final report in 2012.[246] The recommendations in the 2012 Report were

242. *See* 2010 Report, FED. TRADE COMM'N, *supra* note 66, at 39–41; *see also* Edith Ramirez, Commissioner, Fed.Trade Comm'n, Remarks at the Privacy by Design Conference: Privacy By Design and the New Privacy Framework of the U.S. Federal Trade Commission (June 13, 2012) ("In March, the FTC released a final privacy report that clarifies and fine-tunes a framework we first proposed in December 2010. The final FTC report espouses three core principles: privacy by design, simplified choice, and transparency.").

243. 2010 Report, FED. TRADE COMM'N, *supra* note 66, at ix. On the first PbD protection, "data security," the Commission offered little elaboration beyond asserting that companies should employ reasonable safeguards, "including physical, technical, and administrative safeguards," and that the level of security depends on "the sensitivity of the data, the size and nature of a company's business operations, and the types of risks a company faces." *Id.* at 44–45. On the need to impose "reasonable collection limits," the Commission explained that "companies should collect only the information needed to fulfill a specific, legitimate business need," and offered several examples. *See, e.g.*, *id.* ("If a mobile application is providing traffic and weather information to a consumer based on his or her location information, it does not need to collect contact lists or call logs from the consumer's device."). On the point of data retention, the Commission explained that business should retain "consumer data for only as long as they have a specific and legitimate business need to do so," and provided a single example, location-based data, which the FTC said could be especially revelatory about a consumer's personal life. *Id.* at 46–47. On the final protection, data accuracy, the Commission was terse, only asserting that companies should take special care where "such data could be used to deny consumers benefits or cause significant harm." *Id.* at 48.

244. 2010 Report, FED. TRADE COMM'N, *supra* note 66, at 44.

245. *Id.* at iii–v. In the introduction to the report, the Commission identified several "major themes" that emerged from these roundtables:

> [T]he ubiquitous collection and use of consumer data; consumers' lack of understanding and ability to make informed choices about the collection and use of their data; the importance of privacy to many consumers; the significant benefits enabled by the increasing flow of information; and the blurring of the distinction between personally identifiable information and supposedly anonymous or de-identified information.

Id. at iv.

246. 2012 Report, FED. TRADE COMM'N, *supra* note 66, at i.

substantially similar to those in 2010: the Commission proposed the same three-part framework, including the same four PbD "protections," or "substantive principles," plus the "comprehensive data management procedures" requirement designed to "implement the substantive principles."[247]

Although the term "privacy by design" doesn't appear in FTC complaints and consent decrees, it is easy to see the FTC's PbD vision in action in a number of enforcement actions. In its 2012 Report, the Commission cited cases against Facebook and Google as specific examples of how the PbD framework might work in practice.[248] In its case against Google, the Commission's complaint focused on the fact that Google's "Google Buzz" service—a social networking tool launched in 2010—was turned on by default for users of the company's G-Mail email service, and users who elected to turn off Google Buzz were nevertheless enrolled in certain of the service's features.[249] In its case against Facebook, the Commission alleged that Facebook misrepresented the degree to which users' information was kept private.[250]

Both cases eventually settled, and the final consent orders required both companies to implement comprehensive privacy programs which, if they did not perfectly mirror the Commission's PbD directives, were reflective of the Commission's desire that companies be proactive and brought further definition to its PbD vision. Each consent order required:

> *(1) the designation of personnel responsible for the privacy program; (2) a risk assessment that, at a minimum, addresses employee training and management and product design and development; (3) the implementation of controls designed to address the risks identified; (4) appropriate oversight of service providers; and (5) evaluation and adjustment of the privacy program in light of regular testing and monitoring.*[251]

247. *Id.* at vii.

248. *Id.* at 31 ("The Commission's recent settlements with Google and Facebook illustrate how the procedural protections discussed above might work in practice.").

249. *See* Complaint at 2–5, *In re* Google Inc., (F.T.C. October 2011) (No. C-4336), *available at* https://www.ftc.gov/sites/default/files/documents/cases/2011/10/111024googlebuzzcmpt.pdf; *FTC Charges Deceptive Privacy Practices in Googles Rollout of Its Buzz Social Network*, FED. TRADE COMM'N, Mar. 30, 2011, https://www.ftc.gov/news-events/press-releases/2011/03/ftc-charges-deceptive-privacy-practices-googles-rollout-its-buzz (last visited Feb. 15, 2017).

250. *See generally* Complaint at 6, *In re* Facebook, Inc., (F.T.C. July 2012) (No. C4365), https://www.ftc.gov/sites/default/files/documents/cases/2012/08/120810facebookcmpt.pdf.

251. *See* 2012 Report, FED. TRADE COMM'N, *supra* note 66, at 31; *see also FTC Gives Final Approval to Settlement with Google Over Buzz Rollout*, FED. TRADE COMM'N (Oct. 24, 2011), https://www.ftc.gov/news-events/press-releases/2011/10/ftc-gives-final-approval-settlement-google-over-buzz-rollout; Decision and Order at 4–5, *In re* Google Inc., (F.T.C. Oct. 13, 2011) (No. C-4336) [hereinafter *Google Consent Decree*]; Agreement Containing Consent Order at 5–6, *In re* Facebook, Inc., (F.T.C. 2011) (No. C-4365) [hereinafter *Facebook Consent Decree*]; *Facebook Settles FTC Charges That It Deceived Consumers By Failing To Keep Privacy*

As the Commission explained in its 2012 Report, the FTC's orders in each case focus on the companies' duty to implement a comprehensive program designed to assess risk:

> *The FTC's orders will require the companies to implement a comprehensive privacy program reasonably designed to address privacy risks related to the development and management of new and existing products and services and to protect the privacy and confidentiality of "covered information," defined broadly to mean* any *information the companies collect from or about a consumer.*[252]

Notably, the FTC advised that the Google and Facebook settlements are guideposts for companies seeking to implement PbD: "Companies should view the comprehensive privacy programs mandated by these consent orders as a roadmap as they implement privacy by design in their own organizations."[253]

There are other enforcement actions where the Commission's PbD vision is apparent, if not terribly precise or well-defined. Its 2011 complaint against consumer reporting agency ACRAnet, for example, charges the company with failures suggestive of the language in the PbD sections of the 2010 and 2012 Reports and the Facebook and Google settlements.[254] The complaint charges ACRAnet with failure to "develop and disseminate comprehensive information security policies" and "assess the risks of allowing end users with unverified or inadequate security to access consumer reports through ACRAnet's portal."[255] The complaint also cites ACRAnet for failing to conduct risk assessments.[256] Likewise, the FTC's complaints against SettlementOne Credit Corp., Fajilan and Associates, and Lookout Services Inc. allege failures to implement "policies" and "procedures" and "systems" for mitigating cybersecurity risk, and failures to "assess risks" and take steps to address these risks.[257]

Promises FED. TRADE COMM'N (Nov. 29, 2011), https://www.ftc.gov/news-events/press-releases/2011/11/facebook-settles-ftc-charges-it-deceived-consumers-failing-keep.

252. *See* 2012 Report, FED. TRADE COMM'N, *supra* note 66, at 31.

253. *Id.*

254. *See generally* Complaint, *In re* ACRAnet, Inc., (F.T.C. Aug. 17, 2011) (No. C-4331) https://www.ftc.gov/sites/default/files/documents/cases/2011/08/110809acranetcmpt.pdf [hereinafter *ARCAnet Complaint*].

255. *Id.* at 2.

256. *Id.* at 3.

257. *See* Complaint at 2–3, SettlementOne Credit Corp., (F.T.C. Aug. 17, 2011) (No. C-4330), https://www.ftc.gov/sites/default/files/documents/cases/2011/08/110809acranetcmpt.pdf ("Among other things, respondents failed to . . . assess the risks of allowing end users with unverified or inadequate security to access consumer reports through SettlementOne's portal[,] implement reasonable steps to address these risks . . . implement reasonable steps to maintain an effective system of monitoring access to consumer reports by SettlementOne's end users[.]"); Complaint at 2–3, *In re* Fajilan & Assocs., Inc., (F.T.C. Aug. 17, 2011) (No. C-

C. *PbD in* Wyndham *and* LabMD

Indeed the *Wyndham* and *LabMD* cases are illustrative of the FTC's determination to impose its PbD program on companies. The settlement order requires Wyndham to "implement, and thereafter maintain [for 20 years], a comprehensive information security program that is reasonably designed to protect the security, confidentiality, and integrity of Cardholder Data."[258] The order also requires that Wyndham (1) designate employee(s) to be responsible for the security program, (2) conduct a risk assessment focused in part on employee training and vulnerabilities in existing systems, (3) "design and implement[] . . . reasonable safeguards to control the risks identified through risk assessment," as well as "regular[ly] test[] or monitor[] the effectiveness of the safeguards' key controls, systems, and procedures," (4) "develop[] and use reasonable steps to select and retain service providers capable of appropriately safeguarding Cardholder Data," and (5) "evaluat[e] and adjust[] the Hotels' and Resorts' information security program…in light of the results of the testing and monitoring required by [number 3]."[259] In short, these requirements mirror, point for point, those placed on Facebook and Google in 2011.[260]

The parallels between the Commission's pronouncements on PbD and its allegations against LabMD are even more explicit. In its complaint, the Commission alleged that LabMD failed to, for example, implement and maintain a "comprehensive security program," identify "commonly known and foreseeable risks," and "adequately train employees to safeguard personal information," all of which the Commission explicitly mentioned in its 2010 and 2012 reports.[261] Interestingly, the Commission had already identified P2P file-sharing networks as a particular area area of concern in 2010, three years before filing a complaint against LabMD. In its 2010 report, the Commission wrote:

4332), https://www.ftc.gov/sites/default/files/documents/cases/2011/08/110819statewidecmpt.pdf ("Among other things, respondents failed to . . . assess the risks of allowing end users with unverified or inadequate security to access consumer reports through Statewide's portal[,] implement reasonable steps to address these risks[,] . . . implement reasonable steps to maintain an effective system of monitoring access to consumer reports by Statewide's end users[,] . . . take appropriate action to correct existing vulnerabilities or threats[.]").Complaint at 2–3, *In re* Lookout Servs., Inc., (F.T.C. June 15, 2011) (No. C-4326), https://www.ftc.gov/sites/default/files/documents/cases/2011/06/110615lookoutcmpt.pdf ("[F]ailed to implement reasonable policies and procedures for the security of sensitive consumer information collected and maintained by Lookout[,] . . . did not adequately assess and address the vulnerability of Lookout's web application to widely-known security flaws[,] . . . failed to employ sufficient measures to detect and prevent unauthorized access to computer networks.").

258. *Wyndham's Stipulated Order*, *supra* note 191, at 4.

259. *Id.* at 5–6.

260. *See Google Consent Decree*, *supra* note 251, at 4; *Facebook Consent Decree*, *supra* note 251, at 5–6.

261. *See supra* Section III.A.

> *The use of peer-to-peer ("P2P") file-sharing software provides one illustration of how incorporating privacy considerations up-front may work. News reports have indicated that sensitive personal information has been shared via P2P file-sharing networks…. Some of these documents became available because businesses allowed employees to download P2P file-sharing programs onto their work computers without proper controls or supervision. In response to this problem, the Commission sent letters to nearly 100 organizations whose customer or employee information was breached through P2P file-sharing software.*[262]

On the whole, the Commission's case against Wyndham was founded on more egregious behavior—three separate breaches, known and unremedied—than in *LabMD*, where the company was, ostensibly, guilty of a single security failure: the existence of a P2P file-sharing application on an employee's computer.[263] Although the Commission's case does not say so, perhaps, in bringing the case against LabMD, it had the foregoing from the 2010 Report in mind.

D. Practical Recommendations

Anyone who has tried to pin down "Privacy by Design" knows the concept can be slippery. The notion has evolved substantially, and in many different directions, from Cavoukian's seven principles first developed in the '90s. Even the FTC's specific pronouncements in the 2010 and 2012 privacy reports give little guidance on what, exactly, the Commission expects when it requests that companies implement PbD. In this respect, the value of the FTC's complaints and consent orders, in the Google and Facebook cases in particular, cannot be overstated. As discussed above, the Commission imposed several of the same key requirements on the two internet giants.

Previously, the task of sifting through the FTC's cybersecurity settlements was more daunting, but in 2015 the Commission published *Start with Security: A Guide for Business*, which lists ten practical lessons businesses can learn from the FTC's 50+ data security settlements.[264] The following eight recommendations, intended to be more comprehensive, are put forth with those lessons (as well as the Facebook and Google settlements, and the complaints in *Wyndham* and *LabMD*) in mind. In the absence of comprehensive regulation from Congress, businesses that want to avoid the scrutiny of a newly emboldened FTC will, at a minimum, consider the following recommendations:

262. 2010 Report, FED. TRADE COMM'N, *supra* note 66, at 49–50.

263. *See LabMD Complaint, supra* note 3, at 4.

264. *See generally Start with Security*, *supra* note 95.

1. Implement a "Comprehensive" Program

Institute a definite set of policies and procedures designed to address every aspect of the company's data security, and put them in writing.[265] Designate an individual or team to be in charge of the data security program: the higher-ranked those individuals, the better.[266] Indeed, data security should be a discrete and regular topic of discussion for the management team and board members (which discussions should be preserved in meeting minutes). It should also be a priority for all business functions.[267] Instituting comprehensive data security programs can be time consuming and implementing appropriate security measures can be expensive, but do as much as you can reasonably afford. The FTC will expect more from larger, wealthier companies, companies with broad customer bases, and companies that handle especially sensitive data.[268]

2. Get the Basics Right

Although cybersecurity can be complicated, it is not, on the whole, rocket science. Often, data breaches are the result of very basic employee mistakes, or simple, avoidable vulnerabilities exploited by hackers.[269] Require robust login credentials for all employees, including multi-factor authentication measures and complex password requirements.[270] Do not collect more data than you need to,[271] do not keep

265. *See Google Consent Decree*, *supra* note 251, at 4 ("Such program, the content and implementation of which must be documented in writing . . . ."); *Facebook Consent Decree*, *supra* note 251, at 5.

266. *See, e.g.*, *Google Consent Decree*, *supra* note 251, at 4 (Such program . . . shall contain privacy controls and procedures appropriate to respondent's size and complexity, the nature and scope of respondent's activities, and the sensitivity of the covered information . . . .").

267. *See Start with Security*, *supra* note 95, at 2 ("Experts agree on the key first step: Start with security. Factor it into the decision making in every department of your business – personnel, sales, accounting, information technology, etc.").

268. *See, e.g.*, *Facebook Consent Decree*, *supra* note 251, at 5 ("Such program . . . shall contain controls and procedures appropriate to Respondent's size and complexity, the nature and scope of Respondent's activities, and the sensitivity of the covered information[.]"); *see also* Ryan T. Bergsieker et al., *The Federal Trade Commission's Enforcement of Data Security Standards*, 44 THE COLO. LAW. 39, 41 (June 2015) ("More rigorous (and expensive) protections are required of larger organizations possessing large volumes of sensitive information.").

269. *See Start with Security*, *supra* note 95, at 1 ("[L]earning about alleged lapses that led to law enforcement can help your company improve its practices. And most of these alleged practices involve basic, fundamental security missteps.").

270. *See id.* at 4 ("If you have personal information stored on your network, strong authentication procedures – including sensible password 'hygiene' – can help ensure that only authorized individuals can access the data. . . . 'Passwords' like 121212 or qwerty aren't much better than no passwords at all."); Kevin LaCroix, *Cybersecurity Enforcement: The FTC Is Out There*, THE D&O DIARY (Apr. 21, 2015), http://www.dandodiary.com/2015/04/articles/cyber-liability/guest-post-cybersecurity-enforcement-the-ftc-is-out-there. On the password question, the FTC highlights the Twitter action specifically. In the Twitter case, for example, the company let employees use common dictionary words as administrative passwords, as well as

it longer than you need to,[272] and do not give more people access to it than you need to.[273] Encrypt sensitive data.[274] Use firewalls to protect against outsiders and to segment sensitive data within internal systems.[275] Install and update antivirus software on all devices.[276] Implement robust policies for securing remote devices.[277] If someone has published industry-wide standards for your industry, follow them.[278] In light of the *LabMD* case especially, do not allow employees to install P2P software on their computers unless absolutely necessary.[279]

passwords they were already using for other accounts. According to the FTC, those lax practices left Twitter's system vulnerable to hackers who used password-guessing tools, or tried passwords stolen from other services in the hope that Twitter employees used the same password to access the company's system. Twitter could have limited those risks by implementing a more secure password system – for example, by requiring employees to choose complex passwords and training them not to use the same or similar passwords for both business and personal accounts. *Start with Security*, *supra* note 95, at 4. Additionally, user credentials should not be easily accessible on the network. *See id.* at 5 (citing *In re* Guidance Software, Inc., (F.T.C. Mar. 30, 2007) (No. 062-3057)) ("Don't make it easy for interlopers to access passwords. In *Guidance Software*, the FTC alleged that the company stored network user credentials in clear, readable text that helped a hacker access customer credit card information on the network. Similarly, in *Reed Elsevier*, the FTC charged that the business allowed customers to store user credentials in a vulnerable format in cookies on their computers."). Companies should also make sure users are locked out after multiple unsuccessful attempts to log in. *Start with Security*, *supra* note 95, at 5 ("By not adequately restricting the number of tries, the companies placed their networks at risk. Implementing a policy to suspend or disable accounts after repeated login attempts would have helped to eliminate that risk.").

271. *See Start with Security*, *supra* note 95, at 2.

272. *See id.* (citing *In re* BJ's Wholesale Club, Inc., (F.TC. Sept. 23, 2005) (No. C-4148)) ("In the FTC's BJ's Wholesale Club case, the company collected customers' credit and debit card information to process transactions in its retail stores. But according to the complaint, it continued to store that data for up to 30 days – long after the sale was complete. Not only did that violate bank rules, but by holding on to the information without a legitimate business need, the FTC said BJ's Wholesale Club created an unreasonable risk.").

273. *Id.* at 3 ("Not everyone on your staff needs unrestricted access to your network and the information stored on it. Put controls in place to make sure employees have access only on a 'need to know' basis.").

274. *Id.* at 6 ("The method will depend on the types of information your business collects, how you collect it, and how you process it. Given the nature of your business, some possibilities may include Transport Layer Security/Secure Sockets Layer (TLS/SSL) encryption, data-at-rest encryption, or an iterative cryptographic hash."); *see also* Bergsieker, *supra* note 268, at 41 ("Companies must encrypt sensitive data, absent a legitimate reason not to do so.").

275. *See Start with Security*, *supra* note 95, at 7 ("When designing your network, consider using tools like firewalls to segment your network, thereby limiting access between computers on your network and between your computers and the internet.").

276. *Id.* at 8.

277. *Id.*

278. *Id.* at 6 ("When considering what technical standards to follow, keep in mind that experts already may have developed effective standards that can apply to your business. Savvy companies don't start from scratch when it isn't necessary."); *see also* Complaint at 11, United States v. ValueClick, Inc., (C.D. Cal., Mar. 13, 2008) (No. CV08-01711) (alleging that ValueClick "did not use the type of extensively-tested algorithms found in industry-standard systems, but instead utilized a simple alphabetic substitution system that was subject to significant vulnerabilities").

279. *See supra* notes 106 and accompanying text.

3. Conduct Risk Assessments; Test Procedures

The Commission emphasizes that some hacking techniques are well-known and common: these types of threats should be tested for.[280] Testing should also be routine. Just because your security procedures are adequate today, does not mean they will be adequate tomorrow.[281] Update software regularly.[282]

4. Train and Monitor Employees

This is a frequent and vigorous talking point for the Commission.[283] Employees should have easy access to the company's cybersecurity procedures, and should undergo training, not only at the beginning of their employment, but also periodically after they have started working, to ensure they understand the latest IT and cybersecurity developments. Engineers and IT specialists in particular should be trained in secure coding.[284]

5. Ensure That Adequate Protections and Flow-Down Provisions Are Placed on Service Providers

Businesses that have great security policies but fail to adequately verify and monitor the security practices of third party service providers (who often get access to sensitive information) are vulnerable to FTC scrutiny.[285] Obviously, businesses

280. *Start with Security*, *supra* note 95, at 10 ("There is no way to anticipate every threat, but some vulnerabilities are commonly known and reasonably foreseeable. In more than a dozen FTC cases, businesses failed to adequately assess their applications for well-known vulnerabilities.").

281. *See Facebook Consent Decree*, *supra* note 251, at 5–6 ("At a minimum, this privacy risk assessment should include consideration of risks in each area of relevant operation, including, but not limited to: (1) employee training and management, including training on the requirements of this order, and (2) product design, development, and research."); *see also Start with Security*, *supra* note 95, at 12 ("Securing your software and networks isn't a one-and-done deal. It's an ongoing process that requires you to keep your guard up.").

282. *See Start with Security*, *supra* note 95, at 12 ("Outdated software undermines security. The solution is to update it regularly and implement third-party patches.").

283. *See LabMD complaint*, *supra* note 3, at 3 (alleging that LabMD "did not adequately train employees to safeguard personal information"); *see also Start with Security*, *supra* note 95, at 9 ("The company could have reduced the risk of vulnerabilities like that by adequately training its engineers in secure coding practices.").

284. *Start with Security*, *supra* note 95, at 9; *see also* Complaint at 2, *In re* HTC America Inc., (F.T.C. June 25, 2013) (No.122-3049), https://www.ftc.gov/sites/default/files/documents/cases/2013/07/130702htccmpt.pdf (asserting that HTC "failed to implement adequate privacy and security guidance or training for its engineering staff").

285. *Start with Security*, *supra* note 95, at 11 ("When it comes to security, keep a watchful eye on your service providers – for example, companies you hire to process personal information collected from customers or to develop apps."); *see also Google Consent Decree*, *supra* note 251, at 3–4 (requiring Google to acquire consent from consumers, separate from disclosures in its privacy policy and terms of use, before sharing information with third parties); *Facebook Consent Decree*, *supra* note 251, at 6 (requiring "the development and use of reasonable steps to select and retain service providers capable of appropriately protecting the privacy of

cannot control everything third parties do, but they should have third parties agree to security standards in writing, and verify that the third parties are keeping their promises.[286]

6. Fix Problems Quickly

Although the Commission, when applying the unfairness prong of Section 5, is (theoretically) judging whether a company's data security practices are likely to lead to consumer injury (a prospective rather than a retrospective analysis), indeed the FTC's enforcement actions often come on the heels of a cyber breach, and how companies react to those breaches can affect the Commission's and courts' characterizations of the company's security practices.[287] Every company should have a detailed and robust data breach response plan: the plan should be spelled out in the company's data security handbook, and employees should be trained in it as well. Although it can be expensive (for some, prohibitively so), a company that has had a data breach incident should consider retaining experts to help with the response.[288]

7. Publish Accurate Privacy Policies; Stick to Your Promises

Likewise, the unfairness prong analysis does not take promises made in privacy policies and terms of use into account (as the deceptiveness prong analysis does), but, as discussed above, the failure to stick to promises in a privacy policy can not only result in an action based on the deceptiveness prong of Section 5, it can also color a court's thinking on whether a company has been "fair."[289] On this score, the Third Circuit's pronouncement, which for the time being is the highest word on the matter, bears repeating: "A company does not act equitably when it publishes a privacy policy to attract customers who are concerned about data privacy, fails to make good on that promise . . . exposes its unsuspecting customers to substantial financial injury, and retains the profits of their business."[290] You should, in disclosing your practices to consumers, spell out clearly and completely how you handle data (including purposes for which you use the data, how long you keep

covered information they receive from Respondent and requiring service providers, by contract, to implement and maintain appropriate privacy protections for such covered information").

286. *Start with Security*, *supra* note 95, at 11 ("Security can't be a 'take our word for it' thing. Including security expectations in contracts with service providers is an important first step, but it's also important to build oversight into the process.").

287. *See supra* note 73 and accompanying text.

288. *See* Bergsieker, *supra* note 268, at 41 ("Companies need to respond quickly and reasonably to identified vulnerabilities. For example, companies should consider retaining outside experts to address problems that exceed internal capabilities.").

289. *See supra* note 160.

290. *See supra* note 160 and accompanying text.

data, and who has access to it), and do exactly what you say you will.[291] Your privacy policy should be easily accessible and regularly updated to reflect any changes.

8. Show the FTC You're Paying Attention

Finally, it may help if a company can show it has made a good faith effort to examine the FTC's complaints, consent decrees, and publications on data security, and put its recommendations into action. The Commission has a lot of power, but limited resources: close choices between whether to pursue an enforcement action against one company or another could turn on whether the Commission feels the company is listening. Cite FTC documents and consent decrees, and quote specific language in your cybersecurity program. As discussed above, the ten "lessons" from the FTC's 2015 data security guide, as well as the Google and Facebook settlements, should be of special focus.

V. CONCLUSION

It is likely that the final verdict on the FTC's "unfairness" prong tactics has yet to be rendered. Should LabMD ever get a hearing before the appeals court, there are, as discussed above, plenty of facts which could distinguish *LabMD* from the Third Circuit's decision in *Wyndham*. Not bound by Third Circuit precedent, the Eleventh Circuit could even potentially declare the FTC to have exceeded its authority in applying the unfairness doctrine to cybersecurity cases.

In the meantime, the Commission is in the driver's seat. In the absence of comprehensive cybersecurity legislation from Congress, the FTC has become the United States' *de facto* cybersecurity regulator, and its unfairness authority gives the Commission a wide berth to set the boundaries of what constitutes reasonable cybersecurity. Companies desiring to steer clear of the FTC's microscope will, at a minimum, implement the foregoing recommendations, paying special attention, also, to the Commission's publications on cybersecurity, and its settlement decrees in cases against Facebook and Google.

Unfortunately, in spite of what the FTC has spelled out, there are still many unknowns. In a rapidly changing and increasingly interconnected world, this is perhaps to be expected. As malleable and hard to pin down as the "Privacy by Design" concept can be, it is important for companies to at least grasp and adopt the spirit behind it: better to think about privacy first than having to deal with a security breach, and quite possibly the FTC, later.

291. *See Google Consent Decree*, *supra* note 251, at 3 ("[R]espondent . . . shall not misrepresent in any manner, expressly or by implication . . . the extent to which respondent maintains and protects the privacy and confidentiality of any covered information[.]"); *see also Facebook Consent Decree*, *supra* note 251, at 4. The Facebook and Google consent decrees also specifically prohibit certifying participation in a compliance program, such as the U.S.-EU Safe Harbor Framework (since replaced by Privacy Shield). *See supra* note 89.