Volume 61
Issue 6 *V.61, Tolle Lege*

Article 5

6-15-2017

Is The FTC Playing Fair? The Third Circuit's Decision In FTC V. Wyndham Worldwide Corp. Furthers Agency's Data Security Efforts But Creates Tension For Smaller Business

Robert S. Turchick

IS THE FTC PLAYING FAIR? THE THIRD CIRCUIT'S DECISION IN *FTC V. WYNDHAM WORLDWIDE CORP.* FURTHERS AGENCY'S DATA SECURITY EFFORTS BUT CREATES TENSION FOR SMALLER BUSINESSES

ROBERT S. TURCHICK*

"The United States . . . is basically the Wild West of privacy."[1]

I. EVOLVING THREATS: ESCALATING COSTS AND CONSUMER FEARS OVER DATA SECURITY & IDENTITY THEFT

The collection and security of personal information impacts businesses in every market.[2] Personal information is a beneficial resource, but it is also a target for hackers.[3] Data breaches have risen in number from 157 in 2005 to 781 in

* J.D. Candidate, 2017, Villanova University Charles Widger School of Law; B.A., 2012, The Pennsylvania State University. I would like to thank my family for their tireless support and encouragement. I would also like to thank the editors of the *Villanova Law Review* for their feedback on this Casebrief, especially Lauren Anthony, Marie Bussey-Garza, Melissa Ruth, Carina Meleca, John Lisman, Travis Dunkelberger, Marc Robertson, and Allison Sumi Crowe.

1. Joe Nocera, *The Wild West of Privacy*, N.Y. TIMES, Feb. 24, 2014, http://www.nytimes.com/2014/02/25/opinion/nocera-the-wild-west-of-privacy.html?_r=0 [https://perma.cc/5gyx-6b3d] (internal quotation marks omitted) (quoting Barry Steinhardt, Founder, Friends of Privacy USA).

2. *See, e.g.*, *TJX Companies, The, Inc., In the Matter of*, FEDERAL TRADE COMM'N (Aug. 1, 2008), http://www.ftc.gov/enforcement/cases-proceedings/072-3055/tjx-companies-inc-matter [https://perma.cc/29vb-n75f] (directing TJX Companies to implement comprehensive security program designed to protect confidentiality of personal information in response to data breaches occurring between July 2005 and February 2007); *In re* BJ's Wholesale Club, Inc., 140 F.T.C. 465, 471 (2005) (directing BJ's Wholesale Clubs to implement comprehensive security program designed to protect confidentiality of personal information in response to data breaches occurring between November 2003 and February 2004). Despite the FTC's urging, members of Congress are reluctant to rein in the data collection industry on which they increasingly rely to win elections. *See* Evan Halper, *Think Target and Home Depot Invade Your Privacy? Political Campaigns Might Be Worse*, L.A. TIMES (Jan. 27, 2016), http://www.latimes.com/nation/politics/la-na-political-campaign-data-privacy-20160127-story.html [https://perma.cc/6elx-ck2l] (positing that political campaigns may collect "more personal information on Americans than even the most aggressive retailers"); Rosalind S. Helderman, Anne Gearan, & John Wagner, *DNC Penalizes Sanders Campaign for Improper Access of Clinton Voter Data*, WASH. POST (Dec. 18, 2015), https://www.washingtonpost.com/politics/dnc-sanders-campaign-improperly-accessed-clinton-voter-data/2015/12/17/a2e2e14e-a522-11e5-b53d-972e2751f433_story.html [https://perma.cc/3jn4-85zq] (detailing theft of "master voter lists" from DNC).

3. *See* Kathryn F. Russo, *Regulation of Companies' Data Security Practices Under The FTC Act and California Unfair Competition Law*, 23 COMPETITION: J. ANTI. & UNFAIR COMP. L. SEC. ST. B. CAL. 201, 201 (2014) ("Companies are collecting more sensitive personal information about consumers than ever before while hackers are devising new strategies to access this information."); *see also* Drake Mann, Christopher L. Travis, & Don Lloyd Cook, *Data Security and Privacy: More Than I.T.*, 50 ARKANSAS LAW. 14, 17 (2015) ("Before the recent onslaught of computer viruses and data breaches, perhaps no one could be faulted for not having anti-virus software or paying much attention to data security. But now . . . their

2015, nearly a 500% increase.[4] Businesses that suffer data breaches face a costly internal investigation, possible litigation, and reputational harm.[5] As a result, corporate spending on data security swelled to $1.4 billion in 2014, and the average cost per breach in 2015 reached $6.53 million.[6] American consumers are increasingly aware of data security threats, and the Federal Trade Commission (FTC) reports that the most common complaints from consumers are identity theft and fraud.[7] While criminal activity often defeats outdated security measures, poor business practices may also lead to unintentional misuse or loss of sensitive information.[8]

Despite this clear threat, there is currently no uniform standard governing data security.[9] The FTC has attempted to fill this void by filing enforcement actions against companies with inadequate data security practices.[10] Using

---

appearance on any computer is increasingly foreseeable.").

4. *Compare ITRC Breach Statistics 2005–2014*, IDENTITY THEFT RESOURCE CTR., http://www.idtheftcenter.org/images/breach/2005to2015_20160828.pdf [https://perma.cc/sk2f-8tc4] (last visited Jan. 16, 2016), *with ITRC Breach Reports-2015 Year End Totals*, IDENTITY THEFT RESOURCE CTR., http://www.idtheftcenter.org/ITRC-Surveys-Studies/2015databreaches.html [https://perma.cc/af2h-6a82] (last visited Jan. 16, 2016) (showing increase in number of data breaches).

5. *See* Christopher J. Cox & David R. Singh, *Security Breach Notification Laws: Data Privacy Survey 2015*, WEIL iii, http://www.weil.com/~/media/files/pdfs/1502084_security_breach_notification_broch_en_digital_v2.pdf?la=en [https://perma.cc/xu6v-mqad] (last visited Feb. 14, 2016) (explaining potential fallout for companies that fail to protect personal information properly).

6. *See* Evan M. Wooten, *The State of Data-Breach Litigation and Enforcement: Before the 2013 Mega Breaches and Beyond*, 24 COMPETITION: J. ANTI. & UNFAIR COMP. L. SEC. ST. B. CAL. 229, 229 (2015) ("Corporate legal spending on data security in the United States increased from $1 billion in 2013 to $1.4 billion in 2014, and is expected to climb to $1.5 billion in 2015 . . . ."); *see also 2015 Cost of Data Breach Study: United States*, IBM & PONEMON INST. LLC (May 2015), http://public.dhe.ibm.com/common/ssi/ecm/se/en/sew03055usen/SEW03055USEN.PDF [https://perma.cc/b6vw-8c9d] (explaining "total average cost [of data breach in United States] rose to $6.53 million").

7. *See* Kelly M. Jolley & Lindy L. Gunderson, *Data Breach Liability and Notification: What Do You Need to Know?*, 27 S.C. LAW. 44, 45 (2015) (citing Letter from Leslie Rutledge, Attorney Gen., Ark., et al., to Hon. Mitch McConnell, Senate Majority Leader, et al. (July 7, 2015), http://www.naag.org/assets/redesign/files/sign-on-letter/Final%20NAAG%C20Data%C20Breach%C20Notification%Letter.pdf (discussing rise in identity theft, fraud, and consumer anxiety over last fifteen years)).

8. *See generally An Executive Overview of Generally Accepted Privacy Principles*, AM. INST. CERTIFIED PUB. ACCTS., http://www.aicpa.org/InterestAreas/InformationTechnology/Resources/Privacy/GenerallyAcceptedPrivacyPrinciples/DownloadableDocuments/10261378ExecOverviewGAPP.pdf [https://perma.cc/pgw8-s77m] (last visited Jan. 16, 2016) (stating unintentional data loss is likely to occur).

9. *See* Kenneth A. Bamberger & Deirdre K. Mulligan, *Privacy on the Books and on the Ground*, 63 STAN. L. REV. 247, 254 (2011) ("A majority of privacy scholars and advocates . . . contends that the existing patchwork of U.S. regulation fails to ensure across-the-board conformity with the standard measure of privacy protection . . . ."); Jolley & Gunderson, *supra* note 7, at 45 (noting states have implemented different laws).

10. *See FTC Enforcement Actions*, 3 E-COMMERCE & INTERNET L. 27.06 (2015) (describing FTC's strategy of bringing enforcement actions). The Federal Trade Commission Act enables the FTC to prevent "unfair or deceptive practices" by order, injunction, or

enforcement actions has serious implications for regulated businesses; these actions, unlike generally applicable regulations, are binding only on the parties involved.[11] As a result, critics argue that only a "patchwork" of data security standards exist, and businesses do not have fair notice of how the FTC will apply the standards to their own practices.[12] Furthermore, some question whether the FTC has the authority to enforce data security standards at all.[13] Because the agency settles the majority of these cases, the United States District Court for the District of New Jersey and the Third Circuit Court of Appeals were the first federal courts to address this issue in *FTC v. Wyndham Worldwide Corp.*[14] In *Wyndham*, the Third Circuit applied the "vagueness" standard of fair notice and held that the Wyndham Worldwide Corporation's data security measures failed the FTC's three-part test for unfair practices.[15]

The Third Circuit's holding in *Wyndham* is a win for consumers because it gives the FTC flexibility in pursuing evolving threats, while still requiring fair notice for businesses that collect personal information.[16] Contrary to much of the current criticism, FTC data security efforts are neither indiscriminate nor

---

rulemaking. *See* 15 U.S.C. §§ 45(b), 53(b), 57(a)(1)(B) (2012).

11. *Compare* Londoner v. City & Cty. of Denver, 28 S. Ct. 708, 714 (1908) (holding due process affords interested parties opportunity to be heard when rights are affected by state action "commit[ed] to some subordinate body"), *with* Bi-Metallic Inv. Co. v. State Bd. of Equalization, 36 S. Ct. 141, 142 (1915) (holding political process is safeguard against generally applicable laws). The Court put it best in *Bi-Metallic*, a seminal administrative law case:

> General statutes within the state power are passed that affect the person or property of individuals, sometimes to the point of ruin, without giving them a chance to be heard. Their rights are protected in the only way that they can be in a complex society, by their power, immediate or remote, over those who make the rule.

Id.; *see also* Daniel J. Solove & Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, 114 COLUM. L. REV. 583, 607 (2014) (stating consent decrees are more like contracts between agency and corporation than binding precedent).

12. *See* Bamberger & Mulligan, *supra* note 9, at 254 (discussing uncertainty due to lack of uniformity among privacy laws); Gerard M. Stegmaier & Wendell Bartnick, *Another Round in the Chamber: FTC Data Security Requirements and the Fair Notice Doctrine*, 17 J. INTERNET L. 1, 29 (2013) (claiming formal rulemaking provides fair notice benefits that adjudication does not).

13. *See* Seth Northrop, *Is Your Business Ready for FTC Oversight of Data Security?*, PRIVACY ADVISOR (Sept. 21, 2015), https://iapp.org/news/a/is-your-business-ready-for-ftc-oversight-of-data-security [https://perma.cc/mcr3-byu7] (stating question remained whether FTC could regulate data security practices despite broad authority under FTCA).

14. *See* FTC v. Wyndham Worldwide Corp., 799 F.3d 236 (3d Cir. 2015) (affirming district court); *see also* FTC v. Wyndham Worldwide Corp., 10 F. Supp. 3d 602 (D.N.J. 2014), *aff'd*, 799 F.3d 236 (3d Cir. 2015) (denying defendant's motion to dismiss).

15. *See Wyndham*, 799 F.3d at 236 (providing holding of court).

16. *See* Gerald J. Ferguson & Alan L. Friel, *Challenging FTC Regulation of Cyber-Security After* FTC v. Wyndham, DATA PRIVACY MONITOR (Nov. 4, 2015), https://www.dataprivacymonitor.com/cybersecurity/challenging-ftc-regulation-of-cyber-security-after-ftc-v-wyndham [https://perma.cc/v34f-rrxf] (noting *Wyndham* decision is widely regarded as victory for agency); *see also* John K. Higgins, *Court Bolsters FTC's Authority to Regulate Cybersecurity*, E-COMMERCE TIMES (Sept. 16, 2015), http://www.ecommercetimes.com/story/82496.html [https://perma.cc/yy36-k7w5] ("This is a significant victory for the FTC and American consumers." (quoting Alan Butler, Senior Counsel, Electronic Privacy Information Center) (internal quotation marks omitted)).

unpredictable.[17] The agency's choice to pursue individual enforcement actions enables it to respond to constantly-changing cyber threats.[18] By issuing informal guidance and publicizing past enforcement actions, the FTC has provided sufficient notice that a company's data security practices could be challenged as legally unfair.[19] Still, while the *Wyndham* decision aids consumer protection, it raises the question of how smaller companies can keep up with data security developments and the FTC's expectations without going bankrupt.[20] This Casebrief offers advice to compliance officers and legal counsel in the Third Circuit on how to minimize FTC scrutiny in the wake of *Wyndham*.

Part II discusses the Third Circuit's articulation of the fair notice doctrine and the FTC's brief history of enforcing data security standards.[21] Part III discusses the background of *Wyndham*, the Third Circuit's analysis, and why the decision is a victory for consumers, as well as the FTC.[22] Part IV details the pressure that the vagueness standard places on small businesses that collect personal information and suggests basic steps they can pursue to mitigate FTC scrutiny.[23] Part V concludes by stressing the importance of documenting efforts to maintain strong (and "fair") data security practices.[24]

II. ADVANCEMENTS IN JURISDICTION: FTC'S ROLE EVOLVES AFTER DIGITAL REVOLUTION, BUT OLD RULES STILL APPLY

Before initiating enforcement actions, the FTC, like all agencies, must instruct entities collecting personal information on the standards to which they will be held.[25] The broad scope of the Federal Trade Commission Act of 1914 (FTCA) allowed the FTC to emerge as the prominent privacy enforcer in the United States, outside of existing, industry-specific laws.[26] The FTC has fulfilled

17. *See* Solove & Hartzog, *supra* note 11, at 624 ("There have been hardly any noted instances of inconsistency, despite a sizeable number of practitioner commentators who have analyzed FTC cases.").

18. *See id.* at 589 (noting enforcement allows agency to remain "adaptable in the face of technological change").

19. *See id.* at 621 (noting complaints and settlements are made publicly available on FTC's website).

20. *See* Blake Edwards, *Big Law and Big Data: On What's Legal and What's Creepy*, BLOOMBERG (Feb. 5, 2016), https://bol.bna.com/big-law-and-big-data-on-whats-legal-and-whats-creepy [https://perma.cc/97j8-8yz4] (quoting Marc Roth, partner at Manatt, Phelps & Phillips, LLP, on challenges faced by small businesses due to FTC regulations).

21. *See infra* notes 25–93.

22. *See infra* notes 94–137.

23. *See infra* notes 138–153.

24. *See infra* notes 154–157.

25. *See, e.g.*, F.C.C. v. Fox Television Stations, Inc., 132 S. Ct. 2307, 2317 (2012) ("A fundamental principle in our legal system is that laws which regulate persons or entities must give fair notice of conduct that is forbidden or required.").

26. *See* Bamberger & Mulligan, *supra* note 9, at 284–85 (arguing "procedural breadth inherent in the FTC Act" allowed FTC "to play an increasingly important role" in developing online privacy norms); *see also* Solove & Hartzog, *supra* note 11, at 606 (asserting FTC has gradually gained authority over data security in last fifteen years); Stegmaier & Bartnick, *supra* note 12, at 18 (stating FTC has become predominant data security regulator in absence of comprehensive regulatory scheme). However, the FTCA by no means foreshadowed the FTC's

this role for more than a decade by issuing informal guidance and initiating individual enforcement actions against companies with "unfair" data security practices.[27] This approach has been criticized for failing to give notice of what data security standards are required by law, and there are calls for uniform data security regulation.[28] However, the FTC's informal guidance and complaints and settlements stemming from unfair data security enforcement actions demonstrate the agency's consistent expectations regarding data security practices.[29]

A. *Selecting a Firewall: The Third Circuit Enforces the Fair Notice Doctrine*

FTC enforcement actions allow the agency to keep pace with evolving threats, but these enforcement actions raise stronger fair notice concerns than would a formal regulation.[30] Due process requires laws to give fair notice of what conduct is forbidden or required by the government.[31] This doctrine extends to criminal and civil statutes, especially when penalties are imposed for violations.[32]

---

transformation into the country's most prominent privacy regulator. *See* Interview by Vicki Jackson, Professor, Harvard Law Sch., with Joan Z. Bernstein, Dir., Bureau of Consumer Protection, FTC (May 1, 2000), http://www.americanbar.org/content/dam/aba/directories/women_trailblazers/bernstein_historical_society_of_dc_circuit_interview_2.authcheckdam.pdf [https://perma.cc/p9u2-73vn]. Bernstein, who is now in private practice, offered a candid and intriguing perspective of the nascent FTC authority over cybersecurity:

> The one place where there were some very vigorous issues of jurisdiction was in the privacy area. It didn't quite fit into "deception or unfairness" for us to say, "Everybody out there ought to be required to protect people's privacy." Didn't quite fit the jurisdictional model. If you said you were doing something and you didn't do it, we could assert our authority, and we did, using traditional law enforcement. But we couldn't get to the other place. There were internal discussions about how to handle it and from that came our concept of convening forums on privacy issues on the Internet very early and to articulate our program. Then we did the first survey of what was happening to the personal privacy on the web sites, encouraging self-regulation, the privacy issues are real hot right now.

Id.

27. *See* Solove & Hartzog, *supra* note 11, at 624, 627 (arguing "common law of privacy" has emerged from enforcement actions and informal agency activity).

28. *See* Stegmaier & Bartnick, *supra* note 12, at 29 (arguing that regulating data security "through complaints and consent orders . . . creates ambiguity").

29. *See* Solove & Hartzog, *supra* note 11, at 624 (stating enforcement actions have created cognizable standards).

30. *See* Stegmaier & Bartnick, *supra* note 12, at 19 ("An agency using enforcement conduct, rather than less adversarial methods, to define the contours of its broad discretion likely raises greater due process concerns." (citing Martin v. Occupational Health and Review Comm'n, 499 U.S. 144, 158 (1991)).

31. *See* F.C.C. v. Fox Television Stations, Inc., 132 S. Ct. 2307, 2317 (2012) (holding fair notice is fundamental right of all persons); United States v. Williams, 553 U.S. 285, 304 (2008) (requiring fair notice to regulations); Papachristou v. City of Jacksonville, 405 U.S. 156, 162 (1972) (asserting all persons are owed notice of what behavior government requires of them or forbids); Connally v. Gen. Constr. Co., 269 U.S. 385, 390 (1926) (claiming statutes must use words and phrases known well enough to enable persons to apply them correctly).

32. *See Fox Television Stations*, 132 S. Ct. at 2317–20; Theodore J. Boutrous, Jr. & Blaine H. Evanson, *The Enduring and Universal Principle of "Fair Notice"*, 86 S. CAL. L. REV. 193, 196–97 (2013) (noting fair notice applies to "corporate civil defendants facing imposition of civil penalties by regulatory agencies").

Nevertheless, the fair notice requirement for civil statutes may be satisfied with a lower level of specificity because the consequences are less grave.[33] The Third, Fourth, and Fifth Circuits invalidate civil statutes that regulate economic activity as void for vagueness only when the statute is "so vague as to be no rule or standard at all."[34] However, the Third Circuit has held a higher standard of notice—"ascertainable certainty"—is required when an *agency*, rather than a court, interprets the meaning of its own organic statute or regulation because of the high level of deference owed these interpretations.[35]

Fair notice also requires standards to ensure the law's enforcer does not act

---

33. *See* San Filippo v. Bongiovanni, 961 F.2d 1125, 1135 (3d Cir. 1992) ("Lesser degrees of specificity are required to overcome a vagueness challenge in the civil context than in the criminal context, however, because the consequences in the criminal context are more severe." (citing Hoffman Estates v. Flipside, Hoffman Estates, Inc., 455 U.S. 489, 498–99 (1982)).

34. *See, e.g.*, CMR D.N. Corp. v. City of Philadelphia, 703 F.3d 612, 632 (3d Cir. 2013) (quoting Boutilier v. INS, 387 U.S. 118, 123 (1967)) (stating statute is invalid if it fails to give interested parties reasonable notice of what it requires); Mayes v. City of Dallas, 747 F.2d 323, 324 (5th Cir. 1984) (holding detailed criteria set forth in regulation was valid under Fourteenth Amendment); Maher v. City of New Orleans, 516 F.2d 1051, 1062 (5th Cir. 1975) (holding legislature provided "adequate legislative direction" to city's preservation commission to avoid due process violation).

35. *See* Sec'y of Labor v. Beverly Healthcare-Hillview, 541 F.3d 193, 202 (3d Cir. 2008) (noting approval of cases holding "ascertainable certainty" as fair notice standard when agency interprets its own regulation); Dravo Corp. v. Occupational Safety & Health Review Comm'n, 613 F.2d 1227, 1232 (3d Cir. 1980) ("[T]he Secretary as enforcer of the Act has the responsibility to state with ascertainable certainty what is meant by the standards he has promulgated." (quoting Diamond Roofing Co. v. Occupational Safety & Health Review Comm'n, 528 F.2d 645, 645–50 (5th Cir. 1976)); *accord* Nat'l Oilseed Processors Ass'n v. OSHA, 769 F.3d 1173, 1183–84 (D.C. Cir. 2014) (rejecting vagueness claim because words of regulation combined with public guidance from OSHA provided "ascertainable certainty" of standards); Chem. Waste Mgmt. v. E.P.A., 976 F.2d 2, 29 (D.C. Cir. 1992) (citing *Diamond Roofing Co.*, 528 F.2d at 649 (holding agencies have "responsibility" to delineate what standards are required by regulations with "ascertainable certainty"); *Diamond Roofing Co.*, 528 F.2d at 649 (holding regulation did not apply to "open-sided roofs" because OSHA failed to provide "ascertainable certainty" that it did). In the Third Circuit, the "ascertainable certainty" standard is applicable only when:

> (1) the agency had given conflicting public interpretations of the regulation or (2) the regulation is so vague that the ambiguity can only be resolved by deferring to the agency's own interpretation . . . and the agency has failed to provide a sufficient, publicly accessible statement of that interpretation before the conduct in question.

Beverly Healthcare-Hillview, 541 F.3d at 202 (quoting United States v. Lachman, 387 F.3d 42, 57 (1st Cir. 2004)); *see also* Frank H. Easterbrook, *Judicial Discretion in Statutory Interpretation*, 57 OKLA. L. REV. 1, 3 (2004) (explaining agencies and judges interpret statutes differently). Easterbrook notes that agencies are influenced by factors that do not reach the bench, such as political pressure and cost-benefit analyses. *See id.* Because courts will defer to agencies' reasonable interpretations of their organic statutes and regulations in the absence of clear congressional direction, it is important to hold agency outputs to higher standards of fair notice in these contexts. *See* Chevron U.S.A., Inc. v. Natural Res. Def. Council, Inc., 467 U.S. 837, 843 (1984) ("[I]f the statute is silent or ambiguous with respect to the specific issue, the question for the court is whether the agency's answer is based on a permissible construction of the statute."); *see also* Auer v. Robbins, 519 U.S. 451, 457 (1997) (holding Secretary of Labor's reasonable interpretation of regulation denying exempt status to certain employees must be sustained where Congress had not addressed issue); Bowles v. Seminole Rock & Sand Co., 325 U.S. 410, 414 (1945) (holding that administrator's construction of regulation is "of controlling weight unless it is plainly erroneous").

arbitrarily.[36] More serious fair notice concerns arise when an agency pursues its regulatory agenda by using enforcement actions instead of promulgating regulations because the standards will not necessarily consist of authoritative law.[37] In this context, a court may assess the agency's pre-enforcement activities to find that an agency provides fair notice of potential liability.[38] This assessment primarily involves consulting administrative guidance, public statements, reports, and complaints and settlements stemming from enforcement actions.[39] To raise public awareness and "conserve agency resources," the FTC strategically files complaints against large companies with practices that are representative of industry standards.[40] Subsequent settlements are made public in the Federal Register.[41] These settlements are not legally binding to non-parties, but they are frequently treated as "adjudicated precedent" by other companies with similar practices.[42]

B. *Important Notification: The FTCA & Subsequent Congressional Action Suggest FTC Will Regulate Unfair Data Security Practices*

Far from precise, the FTCA gives the FTC broad discretion for determining what constitutes unfair commercial practices.[43] Congress originally created a list of twenty unfair business practices, but omitted these restrictions from the

36. *See* Grayned v. City of Rockford, 408 U.S. 104, 109 (1972) (asserting known standards must set bounds of enforcement).

37. *See* Stegmaier & Bartnick, *supra* note 12, at 19 ("An agency using enforcement conduct, rather than less adversarial methods, to define the contours of its broad discretion likely raises greater due process concerns." (citing Martin v. Occupational Safety and Health Review Comm'n, 499 U.S. 144, 158 (1991)).

38. *See* Gen. Elec. Co. v. E.P.A., 53 F.3d 1324, 1329 (D.C. Cir. 1995) (explaining that "in many cases the agency's pre-enforcement efforts to bring about compliance will provide adequate notice"); Stegmaier & Bartnick, *supra* note 12, at 20 (stating that informal agency outputs such as public statements, consent decrees, and policy statements may factor into fair notice analysis).

39. *See* Sarah Sargent, *Fight or Comply: The Federal Trade Commission's Power to Hold Companies Liable for Data Security Breaches*, 41 J. CORP. L. 529, 539 (2015) (distinguishing guidance and reports from consent decrees).

40. *See id.* (citing Solove & Hartzog, *supra* note 11, at 624).

41. *See id.* (noting both complaints and settlements are published in *Federal Register*).

42. *See id.* (citing Solove & Hartzog, *supra* note 11, at 620).

43. *See* 15 U.S.C. § 45(a)(1) (2012). The FTCA declares unlawful "[u]nfair methods of competition in or affecting commerce" and "unfair or deceptive acts or practices in or affecting commerce." *See id.* The legislative history makes clear that Congress intended for the FTC to use its expertise to determine what constitutes an unfair or deceptive practice. *See* S. REP. NO. 63-597, at 13 (1914) ("The committee gave careful consideration . . . as to whether it would . . . define the many and variable unfair practices . . . or whether it would, by a general declaration condemning unfair practices, leave it to the commission to determine what practices were unfair. It concluded that the latter course would be the better . . . ."); H.R. REP. NO. 63-1142, at 19 (1914) (Conf. Rep.) ("It is impossible to frame definitions which embrace all unfair practices. There is no limit to human inventiveness in this field . . . . If Congress were to adopt the method of definition, it would undertake an endless task."); *see also* Eugene R. Baker & Daniel J. Baum, *Section 5 of the Federal Trade Commission Act: A Continuing Process of Redefinition*, 7 VILL. L. REV. 517, 518 (1962) (discussing broad scope of FTCA as intended by Congress).

statute.[44] Congress reasoned that any number of activities could potentially be deemed unfair and feared that limiting the FTC's ability to regulate novel practices would undermine the statute's basic goal.[45] Rather than consult a discrete list, the FTC uses a three-part test to determine if a commercial practice is unfair.[46] Legally unfair practices are those that (1) cause or are likely to cause substantial injury to consumers or competition, (2) could not have been reasonably avoided, and (3) are not outweighed by countervailing benefits to consumers or businesses.[47] The FTC determines the third factor using a cost-benefit analysis that examines "the cost of available [tools]," the "size and complexity" of the company, and the nature of the business.[48] Since 1980, the agency has openly used this power to strike down business methods in a variety of trades and services, from retail to entertainment.[49]

Decades after the FTCA was passed, the FTC entered the data security field in response to domestic and foreign market pressures in the mid-1990s.[50]

---

44. *See* SEN. REP. NO. 63-597, at 13 (declining to define "unfair practices"); H.R. REP. NO. 63-1142, at 19 (noting constantly evolving practices that could potentially fit within definitional ambit of "unfair practices").

45. *See* S. REP. NO. 63-597, at 13; H.R. REP. NO. 63-1142, at 19 (giving FTC room to combat unfair practices that had not yet been determined).

46. *See* Russo, *supra* note 3, at 202 (noting FTC uses three-part test for unfair practices).

47. *See* Letter from the FTC to Hon. Wendell Ford & Hon. John Danforth, Senate Comm. on Commerce, Sci., and Transp. (Dec. 17, 1980) [hereinafter 1980 Policy Statement]. The 1980 Policy Statement, discussed at length in *Wyndham*, set the modern framework for legally unfair practices:

> To justify a finding of unfairness the injury must satisfy three tests. [1] It must be substantial; [2] it must not be outweighed by any countervailing benefits to consumers or competition that the practice produces; and [3] it must be an injury that consumers themselves could not reasonably have avoided.

Id. This test was subsequently endorsed by the FTC in enforcement actions. *See e.g.*, *In re* Int'l Harvester Co., 104 F.T.C. 949, 102 (1984). This was a departure from previous interpretations of the FTC's "unfairness" authority. *Cf.* 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 1964 Policy Statement]. The 1964 Policy Statement listed the following three factors as guiding an agency's actions under the statute: (1) Whether, without being illegal, the practice "offends public policy" as established by statute, the common law, or other established notions of fairness; "(2) whether it is immoral, unethical, oppressive, or unscrupulous;" and "(3) whether it causes substantial injury to consumers [or businesses]." *See id.* Earlier cases focused on the second factor from the 1964 Policy Statement. *See, e.g.*, FTC v. R.F. Keppel & Bro., Inc., 291 U.S. 304, 313-14 (1934) (stating "unscrupulous" and "unethical" behavior bolsters claim for unfair practices); FTC v. Gratz, 253 U.S. 421, 427 (1920) (noting only practices that were "opposed to good morals" were designated unfair). The Supreme Court held that the second factor could not be used as an independent basis for a finding of unfairness in *FTC v. Sperry & Hutchinson Co.*, 405 U.S. 233, 241–42 (1972).

48. *See* Russo, *supra* note 3, at 202–03 (citing Prepared Statement of the Fed. Trade Comm'n Before the Comm. on Energy & Commerce (Feb. 5, 2014), http://www.ftc.gov/system/files/documents/public_statements/prepared-statement-federaltrade-commission-protecting-consumer-informationcandata-breaches-be/140205databreaches.pdf) (explaining flexibility of third factor).

49. *See* 1980 Policy Statement, *supra* note 47; *see also In re* Dave & Buster's, Inc., 149 F.T.C. 1449 (2010) (applying three-part test to entertainment industry); *In re* DSW Inc., F.T.C. No. C-4157, 2006 WL 752215 (F.T.C. Mar. 7, 2006) (applying three-part test to shoe retail industry).

50. *See* Solove & Hartzog, *supra* note 11, at 590 (discussing American public's

Awareness and fear surrounding personal information-gathering strengthened as the digital revolution progressed in the new millennium.[51] While Congress intended for the scope of "unfair practices" to be indefinite, the legislature has directed several agencies to regulate data security in specific industries such as healthcare, children's websites, credit reporting, and financial services.[52]

Of the these specific grants, the Gramm-Leach-Bliley Act (GLB) and its related regulations provide the most stringent standards for data security, and they are often used by the FTC in settlements as a model for mandated compliance programs.[53] The statute's "safeguard" provision includes protection requirements for "customer records," protecting against "anticipated [security] threats or hazards," and preventing the "unauthorized access to . . . such [] information."[54] The FTC also directs financial institutions to designate at least one employee to coordinate an information program and identify reasonably foreseeable internal and external threats to the security and confidentiality of

"reluctan[ce] to use the Internet out of fear that their data could be improperly accessed" in "mid-to-late 1990s"); *see also* Bamberger & Mulligan, *supra* note 9, at 284–85 (2011) (explaining pressure on United States to improve data privacy laws after European Union passed Data Protection Directive in 1995). The Data Protection Directive prohibited European companies from sending data to companies in nations with what the European Union deemed inadequate privacy laws. *See id.* (citing Directive 95/46/EC, 1995 O.J. (L 281) 31). The Directive states that "personal data may only be transferred to parties in a third country if that country provides an 'adequate level of protection.'" *Id.* n.59 (citing Directive 95/46/EC, 1995 O.J. (L 281) at 45). As a result, data protection became a major trade issue for the Clinton administration, and U.S.-based multinational companies "feared the economic consequences" of lax privacy standards. *See id.* at 283–85. In response to these fears, the United States and European Union agreed to the Safe Harbor Privacy Principles in 2000, which allowed U.S. companies to "self-certify" that their data security measures were "sufficient for trade with European partners." *See id.* at 285. A significant caveat to this agreement was a mandate that the FTC "enforce privacy [policies]" that are claimed by American companies. *See id.* The agreement somewhat shielded the FTC from criticism that its burgeoning involvement in data security was "beyond its inherent authority." *See id.* at 285–86.

51. *See* Editorial Board, Op-Ed, *Consumers Should Be Able to See the Data Companies Collect About Them*, WASH. POST (May 31, 2014), https://www.washingtonpost.com/opinions/consumers-should-be-able-to-see-the-data-companies-collect-about-them/2014/05/31/82a821cc-e819-11e3-8f90-73e071f3d637_story.html [https://perma.cc/cer7-kshq] (alluding to more invasive personal information collection by private sector as consequence of "digital revolution").

52. *See, e.g.*, Children's Online Privacy Protection Act, Pub. L. 105-277, § 1303, 112 Stat. 2681, 2681 (1998) (codified at 15 U.S.C. § 6502) [hereinafter COPPA]. COPPA requires the operator of a children's website to provide notice to users of what information is being collected and how it is used. *See id.* § 6502(a)(1) ("It is unlawful for an operator of a website or online service directed to children . . . to collect personal information from a child in a manner that violates the regulations prescribed . . . ."); *see also* Fair and Accurate Credit Transactions Act, Pub. L. No. 108-159, § 216(a), 117 Stat. 1952, 198-86 (2003) (codified at 15 U.S.C. § 1681(w) (2012)) [hereinafter FACTA]. FACTA contains provisions to help reduce identity theft stemming from stolen credit reports. *See id.* § 1681(w). It directs the FTC and several other agencies to issue final regulations requiring credit reporting agencies to safely dispose of consumers' credit information. *See id.*; *see also* Proper Disposal of Consumer Information, 69 Fed. Reg. 35496 (June 24, 2004) (codified at 16 C.F.R. § 682.3 (2016)).

53. *See* Pub. L. No. 106-102, § 501(b), 113 Stat. 1338, 1436–37 (1999) (codified at 15 U.S.C. § 6801(b) (2012)); *see also FTC Enforcement Actions*, *supra* note 10 (noting similarity between GLB compliance and FTC data enforcement settlements).

54. *See* Fair Credit Reporting Act, 15 U.S.C. § 6801(b) (2012).

consumer information.[55] At a minimum, this risk assessment should include consideration of existing "employee training and management . . . network and software design . . . information processing . . . and disposal[,] [] and detecting and preventing" foreseeable threats.[56] The FTC also calls on financial institutions to "regularly test" and improve the effectiveness of their security procedures in response to new risks.[57]

C. *FTC Publicizes Data Security Standards & How It Will Respond to Unfair Practices*

A review of the FTC's pre-enforcement activities gives companies fair notice that their data security standards may be challenged. The FTC issued public statements on best privacy practices, even before its first unfair data security enforcement action.[58] Although these statements do not have the force and effect of law, they present a strong case for fair notice when considered along with the FTC's fifty-plus settlements since 2005.[59] While not precise, FTC publications and allegations set forth in the FTC's unfair data security complaints have been very consistent.[60] These publicly available resources provide perceptive companies an outline for avoiding scrutiny.[61]

1. *Download Optional: FTC Offers Guidance, but Businesses Technically Are Not Obligated to Follow*

In 2003, former FTC Commissioner Orson Swindle testified before the House Commerce, Trade, and Consumer Protection Subcommittee regarding the importance of a "culture of security" in a computer-driven economy.[62] In his

55. *See* Standards for Safeguarding Customer Information, 67 Fed. Reg. 36493 (May 23, 2002) (codified at 16 C.F.R. § 314.4(a)–(b) (2016)) (listing elements of appropriate security program).

56. *See* 16 C.F.R. § 314.4(b). At a minimum, the risk assessment should consider new employee training and management procedures. *See id.* § 314.4(b)(1). It should also consider new information systems. *See id.* § 314.4(b)(2). Finally, it must consider how threats are detected and prevented. *See id.* § 314.4(b)(3).

57. *See id.* § 314.4(c) (requiring parties to "[d]esign and implement information safeguards to control the risks [they] identify through risk assessment, and regularly test or otherwise monitor the effectiveness of the safeguards' key controls, systems, and procedures").

58. *See* Bamberger & Mulligan, *supra* note 9, at 287 (including "best-practice" guidance in list of FTC's important regulatory tools "outside the enforcement context").

59. *See* Skidmore v. Swift & Co., 323 U.S. 134, 140 (1944) (explaining agency interpretations, such as guidelines, are not controlling law and deserve deference insofar as they reflect agency's experience and informed judgment); *see also* Commission Statement Marking the FTC's 50th Data Security Settlement, FED. TRADE COMM'N (Jan. 31, 2014), https://www.ftc.gov/system/files/documents/cases/140131gmrstatement.pdf [https://perma.cc/llj2-5ewx] (discussing FTC's fiftieth unfair data security practices settlement).

60. *See* Solove & Hartzog, *supra* note 11, at 620 (stating FTC has been "consistent in [data security] practice" despite not being required to do so).

61. *See id.* (arguing "common law" of privacy provides guidance to regulating entities).

62. *See Cybersecurity and Consumer Data: What's at Risk for the Consumer?: Hearing Before the Subcomm. on Commerce, Trade, and Consumer Prot. of the H. Comm. on Energy and Commerce*, 108th Cong. 14 (2003) [hereinafter *Cybersecurity and Consumer Data*

statement, he said the reasonableness of safety measures should be determined by the nature of a company's business, its size and complexity, and the sensitivity of the information it collects.[63] Furthermore, Swindle recognized that breaches may occur even when all reasonable action has been taken and that not all breaches deserve punishment.[64] He concluded by stating that security is an ongoing process that needs regular monitoring and reevaluation to keep pace with emerging technologies.[65] Since these statements, the FTC has issued informal, but key guidance that has been a catalyst for businesses to implement stronger data security procedures.[66]

Beginning in 2007, the FTC first published its expected standards for protecting sensitive data in *Protecting Personal Information: A Guide for Business*.[67] While the FTC's specific standards depend on the type and size of the business, the FTC calls on any office maintaining personal information to secure and dispose of it safely.[68] The guidebook presents a checklist of smart security practices and encourages the development of training programs that educate employees who handle consumer data like "Social Security numbers, credit card [numbers]," financial account numbers, and other sensitive information.[69] The FTC updated the guidebook in November of 2011 to reflect evolving practices.[70] More recently, in June 2015, the FTC created a new framework known as *Start with Security: A Guide for Business*, which incorporates "lessons learned from FTC cases" with previous material.[71] These pre-enforcement activities provide businesses with a roadmap for avoiding FTC

Hearing] (statement of Orson Swindle, Federal Trade Comm'r, stating importance of compliance with data security standards); *Protecting Info. Sec. & Preventing Identity Theft: Hearing Before the Subcomm. on Tech., Info. Policy, Intergovernmental Relations, & the Census of the H. Comm. on Gov't Reform*, 108th Cong. 6 (2004) (statement of Federal Trade Comm'r Orson Swindle).

63. *See Cybersecurity and Consumer Data Hearing*, *supra* note 62, at 8 (explaining cost-benefit analysis involved in developing strong data security practices).

64. *See id.* at 3 (stating not all breaches deserve punishment, especially when company takes reasonable steps).

65. *See id.* at 12–13 (stating data security practices require constant reevaluation).

66. *See FTC Enforcement Actions*, *supra* note 10 (stating informal guidance has encouraged businesses to improve data security measures); Russo, *supra* note 3, at 201 (stating informal guidance has influenced businesses).

67. *See* FTC v. Wyndham Worldwide Corp., 799 F.3d 236, 256 (3d Cir. 2015) (noting guidebook has been available since 2007).

68. *See id.* at 256–57 (discussing checklist of best practices found in guidebook).

69. *See generally* FED. TRADE COMM'N, PROTECTING PERSONAL INFORMATION: A GUIDE FOR BUSINESS (2016), https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf [https://perma.cc/q7qf-36xx] (listing examples of best practices).

70. *See* Kathleen Rice, Leita Walker & Mary Bono, *FTC Releases Data Security Guide for Businesses*, FAEGRE BAKER DANIELS (July 14, 2015), http://www.faegrebd.com/ftc-releases-data-security-guide-for-businesses [https://perma.cc/t8vn-splq] (noting "latest FTC guidance builds on its 2007 brochure, *Protecting Personal Information: A Guide for Business*").

71. *See* FED. TRADE COMM'N, START WITH SECURITY: A GUIDE FOR BUSINESS, LESSONS LEARNED FROM FTC CASES (2015), https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf [https://perma.cc/n4rh-8cn9] (examining various FTC data breach enforcement actions).

scrutiny.[72]

2. *Responding to Malware: The FTC's Ex Ante Response to Unfair Security Measures Since 2005*

The prospect of an enforcement action looms large for a company that fails to follow administrative guidance.[73] The FTC began by pursuing "deceptive" privacy statements, but, for over a decade, the agency has invoked its "unfairness" authority alone to challenge insufficient data security practices.[74] Companies can expect the FTC to pursue enforcement actions aggressively and require measures that are "reasonable and appropriate under the circumstances."[75] When considering past enforcement actions, a core set of allegations emerges: failing to (1) install "readily available protections, such as firewalls[,] to limit access" to computer networks, (2) "[s]tore[] sensitive [] data" in encrypted form, (3) "remedy known security vulnerabilities," (4) use complex "log-in credentials," (5) "employ reasonable measures to detect and prevent [breaches]," (6) properly respond to security incidents, and (7) "restrict third-party access" to corporate networks adequately.[76] Almost all cases have ended with settlements that require companies to establish a comprehensive security program and submit to third-party auditing "on a biannual basis . . . for a period of time ranging from [ten] to [twenty] years."[77] Notably, the FTC has made these settlements public, providing guidance to companies with similarly unfair practices.[78]

---

72. *See* Solove & Hartzog, *supra* note 11, at 625–26 (noting FTC publishes guidelines with suggestions for best privacy practices).

73. *See* Bamberger & Mulligan, *supra* note 9, at 305, 310 (stating "threat of enforcement" is often necessary to effect "internal change" by regulated businesses).

74. *See FTC Enforcement Actions*, *supra* note 10 (noting FTC's decade-long practice of challenging unfair data security practices); Russo, *supra* note 3, at 201 (discussing FTC's practice of bringing enforcement actions); *see also* Ryan T. Bergsieker, Richard H. Cunningham, & Lindsey Young, *The Federal Trade Commission's Enforcement of Data Security Standards*, 44 COLO. LAW. 39, 39–40 (2015) (explaining FTC's move from challenging solely deceptive privacy practices to challenging insufficient practices as unfair).

75. *See FTC Enforcement Actions*, *supra* note 10 (arguing FTC will pursue enforcement actions); Russo, *supra* note 3, at 204 (suggesting FTC will "continue to aggressively pursue [enforcement] actions"); *see also* REUTERS, *Obama Budget Proposal Includes $19 Billion for Cybersecurity*, FORTUNE (Feb. 9, 2016), http://fortune.com/2016/02/09/obama-budget-cybersecurity [https://perma.cc/d8db-zwz4] (discussing President Obama's Cybersecurity budget proposal). President Obama has asked for a $5 billion increase in the federal government's cybersecurity budget, calling cyber threats an "urgent danger[] to . . . national security". *See id.*

76. *See* Jason Straight, *FTC v. Wyndham: "Naughty 9" Security Fails to Avoid*, INFO. WEEK, http://www.darkreading.com/attacks-breaches/ftc-v-wyndham-naughty-9-security-fails-to-avoid-/a/d-id/1322340 [https://perma.cc/9ku2-aege] (last visited Feb. 14, 2016) (internal quotation marks omitted) (listing failures on part of companies obtained from FTC data security complaints). While the main text mentions numerous "security fails," there are even more potential security mistakes that may put companies at risk of facing an enforcement action. *See id.* (detailing nine potential failures in protecting information).

77. *See* Russo, *supra* note 3, at 204 (noting prevalence of third-party auditing in data security settlements); *see also FTC Enforcement Actions*, *supra* note 10 (discussing common traits of FTC data security enforcement action settlements).

78. *See FTC Enforcement Actions*, *supra* note 10 (noting settlements are public); Russo,

After suffering a breach costing customers $14 million in fraudulent charges, BJ's Wholesale Club (BJ's) became the first company to have its data security practices challenged by the FTC solely on the basis of the agency's unfairness authority.[79] The FTC determined BJ's failed to encrypt information stored on in-store computers, "use readily available security measures," use "sufficient measures to detect" and analyze security breaches, or encrypt information that could be accessed anonymously.[80] The FTC concluded that these practices, when taken together, did not provide adequate protection to consumers.[81] As a result, the FTC alleged BJ's failure to employ sufficient security measures "cause[d] substantial injury to consumers that [was] not offset by countervailing benefits to consumers or competition and [was] not reasonably avoidable by consumers."[82] BJ's agreed to a settlement that included establishing an information security program and submitting to external auditing for a period of twenty years, closely mirroring the compliance requirements of Gramm-Leach-Bliley.[83] Challenges to other companies such as DSW, TJX Companies, Dave & Buster's, and GMR Transcription Services have resulted in similar settlements.[84]

---

supra note 3, at 203 (noting FTC settlements disclosed to public).

79. *See* Consent Order, BJ's Wholesale Club, Inc., 140 F.T.C. 465, 476 (2005) (noting allegation of "substantial consumer injury" caused by breach); Lisa Jose Fales & Jennifer T. Mallon, *The FTC's Use of Its Unfairness Jurisdiction in Data Breach Cases: Is It Fair?*, SECURE TIMES, at 2 (2006), https://www.venable.com/files/Publication/234eeda6-a32d-4dbd-92c9-c463c8e4df99/Presentation/PublicationAttachment/52452d44-e6af-44ec-9709-a534e3e9dcb3/1520.PDF [https://perma.cc/ty6w-pwje] (discussing BJ's data breach).

80. *See In re BJ's Wholesale Club*, 140 F.T.C. at 467 (discussing failures to protect private information). The FTC alleged that BJ's failed to use "reasonable and appropriate" measures to protect consumers' information that was "collected at its stores." *See id.* "Beginning in late 2003 and early 2004, banks began discovering fraudulent purchases that were made using counterfeit copies of credit and debit cards the banks had issued to customers [that had been used at BJ's]." *Id.* As a result, banks and customers had to cancel and re-issue/re-order thousands of credit and debit cards. *See id.*

81. *See id.* (discussing BJ's data security measures pre-breach).

82. *See id.* at 468 (discussing BJ's customers' inability to avoid injury).

83. *See id.* at 471–73 (ordering BJ's take certain measures to ensure future safety of customer information). The steps required of BJ's in the consent order are nearly identical to the regulation promulgated by the FTC in response to GLB. *Compare id.*, *with* 16 C.F.R. § 314.4 (2016) (listing elements of sound "information security program").

84. *See* Consent Order, *In re* DSW Inc., F.T.C. No. C-4157, 2006 WL 752215 (F.T.C. Mar. 7, 2006) (discussing unfair practices of DSW). The FTC alleged that DSW engaged in multiple practices that, when taken together, constituted unfair practices. *See id.* at 2. Among other things, the FTC alleged that DSW

> (1) created unnecessary risks to the information by storing it in multiple files even when it [was no longer needed]; (2) did not use readily available security measures . . . ; (3) stored the information in unencrypted files . . . ; (4) did not limit sufficiently the ability of computers on one in-store network to connect to computers on other . . . networks; and (5) failed to employ sufficient measures to detect unauthorized access.

Id. "The breach compromised a total of approximately 1,438,281 credit and debit cards . . . as well as 96,385 checking accounts and driver's license numbers." *Id.* at 3. The Commission ordered DSW was required to set up a system for testing its security program and was forced to submit to external audits periodically over twenty years, similar to the consent order in *In re BJ's Wholesale Club*. *See id.* at 5. TJ Maxx found itself in a similar situation just two years later. *See In re* TJX Companies, Inc., F.T.C. No. C-4227, 2008 WL 3150421 (F.T.C. July 29,

More recently, the FTC challenged the security practices of LabMD, a cancer-testing laboratory.[85] LabMD "conducted clinical laboratory tests on physical [specimens from patients]" and reported the results to the patients' healthcare providers, and, in doing so, obtained a host of sensitive information.[86] The FTC alleged that, as a result of multiple LabMD security practices that were unfair, the personal information of 9,300 patients was stolen and made available in a public file-sharing network (LimeWire).[87] The FTC filed an administrative complaint in August of 2013.[88]

Rather than settle, LabMD decided to fight back.[89] The administrative law

---

2008). The FTC alleged that information associated with tens of millions of unique payment cards was stolen as a result of TJX's lax security measures. *See id.* at *2. Among its alleged failures, TJX

> (a) created an unnecessary risk to personal information by storing it on and transmitting it . . . in clear text, (b) did not use readily available security measures to limit wireless access to its networks, thereby allowing an intruder to connect wirelessly to in-store networks . . . (c) did not require network administrators and other users to use strong passwords or to use different passwords to access [] programs, computers, and networks, (d) failed to use . . . a firewall . . . ; and (e) failed to employ sufficient measures to detect and prevent unauthorized access to computer networks.

Id. TJX was ordered to establish a security program and submit to external auditing for twenty years. *See id.*; *see also In re* GMR Transcription Servs., Inc., F.T.C. No. C-4482, 2014 WL 4252393 (F.T.C. Aug. 14, 2014) (finding GMR liable for unfair practices similar to those conducted by TJX); Consent Order *In re* Dave & Buster's, Inc., 149 F.T.C. 1449 (2010) (same).

85. *See generally* Complaint, *In re* LabMD Inc., F.T.C. No. 9357, 2013 WL 5232775 (F.T.C. Aug. 29, 2013) (alleging unfair data security practices by Georgia-based cancer research clinic).

86. *See id.* at *1–2 (discussing nature of LabMD's business).

87. *See id.* at *2 (discussing unfair practices). The FTC alleged that LabMD engaged in unfair practices because it:

> (a) did not develop, implement, or maintain a comprehensive information security program to protect consumers' personal information . . . ; (b) did not use readily available measures to identify [problems] . . . ; (c) did not . . . prevent employees from accessing personal information not needed to perform their jobs; (d) did not adequately train employees to safeguard personal information; (e) did not require employees, or other users with remote access to the networks, to use common authentication-related security measures . . . ; and (f) did not maintain and update operating systems of computers and other devices on its networks.

Id. at *3. The *LabMD* case is the most alarming FTC enforcement action brought under the FTCA's unfairness provision because "LabMD had never been [accused of] a HIPAA violation." *See* Cheryl Conner, *When the Government Closes Your Business*, FORBES, (Feb. 1, 2014), http://www.forbes.com/sites/cherylsnappconner/2014/02/01/when-the-government-closes-your-business/#425c908a3652 (providing example of FTC regulating security procedures). The actual breach seems much less dramatic than the systemic failure alleged in the FTC's complaint. *See id.* An employee downloaded the public file-sharing program LimeWire to a work computer, and the sensitive information preserved by LabMD migrated to publicly accessible forums by way of LimeWire's "peer sharing protocol." *See id.* A simple policy of not downloading peer-to-peer file-sharing programs to work computers could have prevented this particular breach. *See id.* However, this Casebrief does not aim to trivialize the LabMD breach, which should have been avoided, and the author is aware that the hypothesized policy might be ineffective without sensible security measures. For a discussion on some of the steps businesses may take to improve data security, see *infra* notes 142–57.

88. *See* Complaint, 2013 WL 5232775, at *3 (alleging unfair data security practices).

89. *See* Respondent LabMD's Motion to Dismiss Complaint with Prejudice and to Stay

judge (ALJ) applied the three-factor unfairness test to LabMD's practices and dismissed the complaint without making a legal conclusion regarding the FTC's jurisdiction.[90] The FTC, which based its theory of injury solely on patients' embarrassment, failed to show tangible injuries.[91] Absent a showing of probability of other harms, the ALJ determined that the FTC failed to show LabMD's practices would "[cause] or [were] likely to cause substantial injury."[92] This result came too late for LabMD; the company closed in 2014 due to litigation costs and the financial burden of the FTC's prospective compliance program.[93]

III. THE CASE IN BRIEF: *FTC V. WYNDHAM WORLDWIDE*

A. *Background & Procedure*

The Wyndham Worldwide (Wyndham) franchise operates hotels and "sells timeshares through three subsidiaries" around the world.[94] It has "licensed its brand name to approximately [ninety] independently owned hotels" and requires each hotel to have "a property management system that processes [customer] information."[95] These systems are "configured" to Wyndham's custom

Administrative Proceedings at 18, *In re* LabMD Inc., F.T.C. No. 9357 (F.T.C. Nov. 12, 2013), https://www.ftc.gov/sites/default/files/documents/cases/131112respondlabmdmodiscomplaintdatyadminproceed.pdf [https://perma.cc/w5ne-efdv] (arguing that, because Congress gave specific grants of data security jurisdiction elsewhere, FTC lacks power to regulate data security through unfairness power).

90. *See* Initial Decision by D. Michael Chappell, Chief Admin. Law Judge, *In re* LabMD Inc., F.T.C. No. 9357, 2015 WL 7575033, at *36–37 (F.T.C. Nov. 13, 2015) (citing Order Denying Respondent LabMD's Motion to Dismiss at 5, LabMD, F.T.C. No. 9357 (F.T.C. Jan. 16, 2014) (refusing to revisit issue of FTC's jurisdiction in initial decision), *vacated*, F.T.C. No. 9357, 2016 WL 4128215 (F.T.C. July 28, 2016) [hereinafter *LabMD* Initial Decision]. The FTC predictably vacated the ALJ's initial finding. *See LabMD Inc.*, 2016 WL 4128215, at *32. While the ALJ determined that a disclosure resulting in a mere risk of harm to consumers was not sufficient to support a finding of unfairness, the FTC ruled that the disclosure alone represented sufficient consumer harm. *See id.* at *8 (opining that disclosure of medical information, while intangible, is "very real harm"). The FTC cited *Wyndham* for the proposition that the fact that a "'company's conduct was not the most proximate cause of an injury generally does *not* immunize liability from foreseeable harms.'" *See id.* at *9 (emphasis added) (quoting *F.T.C. v. Wyndham Worldwide Corp.*, 799 F.3d 236, 246 (3d Cir. 2015)). However, by relying on the *Wyndham* holding in its *LabMD* order, the FTC failed to distinguish between two drastically different factual scenarios and companies. *See infra* notes 119–26 and accompanying text.

91. *See LabMD* Initial Decision, 2015 WL 7575033, at *87 (noting "evidence fails to prove that Respondent's alleged unreasonable data security caused, or is likely to cause, substantial injury to consumers").

92. *See id.*, at *14 ("Fundamental fairness dictates that demonstrating actual or likely substantial consumer injury under Section 5(n) requires proof of more than the hypothetical or theoretical harm . . . .").

93. *See* Conner, *supra* note 87 (quoting LabMD's former CEO).

94. *See* FTC v. Wyndham Worldwide Corp., 799 F.3d 236, 240 (3d Cir. 2015) (discussing nature of Wyndham's business).

95. *See id.* (explaining Wyndham's corporate structure and certain requirements for its properties). Information collected and maintained by these systems "includes [customer] names, home addresses, email addresses, telephone numbers, payment card account numbers, expiration dates, and security codes." *See id.*

specifications.[96] Additionally, Wyndham controls a central computer network in Phoenix, Arizona "that connects . . . with all of the property management systems of each of the Wyndham-branded hotels."[97] Between April 2008 and December 2009, Wyndham's computer system was hacked three times.[98] As a result, the personal and financial information of approximately 619,000 consumers was stolen, leading to "at least $10.6 million in fraud loss."[99]

The FTC filed a complaint against Wyndham in June 2012, claiming "that Wyndham's conduct was an unfair practice and that its [advertised] privacy policy was deceptive."[100] The United States District Court for the District of New Jersey denied Wyndham's motion to dismiss both claims.[101] However, the district court "certified its decision on the unfairness claim for interlocutory appeal."[102] Therefore, the Third Circuit was limited to considering whether the FTC has jurisdiction to regulate data security under the unfairness prong of section 45(a) of the FTCA and, if so, whether Wyndham had fair notice of its data

96. *See id.* (referring to information provided in complaint and discussing Wyndham's computer network infrastructure).

97. *See id.* (explaining connectivity of Wyndham's many property management systems).

98. *See id.* The first attack allegedly occurred in April 2008. *See id.* at 241. Hackers broke into the local network of a hotel in Phoenix by "repeatedly guessing users' login [names] and passwords." *See id.* at 242. The hackers gained "access to an administrator account." *See id.* Next, the hackers stole "unencrypted information for over 500,000 accounts, which they sent to a domain in Russia." *See id.* The second attack occurred in March 2009 when hackers "accessed Wyndham's network through an administrative account." *See id.* According to the FTC, "Wyndham was unaware of the attack for two months until consumers filed complaints about fraudulent charges." *See id.* "[U]nencrypted payment card information for approximately 50,000 customers [was stolen] from the property management systems of [thirty-nine] branded hotels." *See id.* Afterwards, Wyndham found the same "memory-scraping malware used in the previous attack on more than thirty hotels' computer systems." *See id.* Finally, at the end of 2009, hackers accessed another administrator's account, and the "payment card information for approximately 69,000 customers from the property management systems of [twenty-eighty] hotels" was stolen. *See id.* Further, Wyndham was unaware of this attack until January 2010, "when a credit card company received complaints [about fraudulent charges] from cardholders." *See id.*

99. *See id.* at 240–42 (discussing harm to consumers due to Wyndham's multiple breaches).

100. *See id.* at 240 (stating reasoning for FTC's complaint). The FTC's complaint contained seven primary claims: (1) Wyndham maintained payment card information in "clear readable text" files; (2) "Wyndham allowed the use of easily guessed passwords to access the property management systems"; (3) "Wyndham failed to use readily available security measures—such as firewalls—to limit [network] access"; "(4) "Wyndham allowed hotel property management systems to connect to its [main] network [in Phoenix] without taking appropriate cybersecurity precautions"; (5) Wyndham did not "[properly] restrict the [network] access of third-party vendors"; (6) Wyndham "failed to [use] reasonable measures to detect and prevent unauthorized [network] access"; and (7) Wyndham "did not follow proper incident response procedures." *See id.* at 240–41 (internal quotation marks omitted) (citing FTC Complaint).

101. *See id.* at 240, 242 (noting district court's denial of motion to dismiss). The FTC filed suit in the United States District Court for the District of Arizona, but Wyndham successfully requested the case be transferred to the District of New Jersey. *See id.* at 242.

102. *See id.* at 242 (explaining procedural history in district court).

security obligations.[103]

B. *The Third Circuit Breaks Through Wyndham's Weak Arguments*

The Third Circuit ruled against Wyndham on both issues.[104] According to Wyndham, the word "unfair" added additional requirements to the agency's three-part test, such as "unethical behavior."[105] The Third Circuit disagreed because the idea that a company's behavior must be "unscrupulous" or "unethical" to be unfair, even though unfair practices *may* be unethical, has long been rejected.[106] Having determined that Wyndham's data security practices fell within the purview of the FTCA, the Third Circuit applied the three-part unfairness test to Wyndham's data breach.[107] The court found significant and quantifiable consumer injury in the form of $10.6 million suffered by Wyndham customers due to fraudulent charges from the breaches.[108] Moreover, the court reasoned that because Wyndham had advertised data security measures on par with industry standards, customers were deceived and could not avoid losing their personal information.[109] Lastly, one should note that, given Wyndham's size and multiple data breaches, improving safeguards would not have presented countervailing burdens to consumers or the business that outweighed the benefits of better data security practices.[110]

Next, the Third Circuit held that Wyndham was not owed "ascertainable certainty" of the FTC's position on what data security measures "are required by [section] 45(a)" of the FTCA.[111] In the absence of an FTC regulation, the court

---

103. *See Wyndham*, 799 F.3d at 240 (noting issues under consideration). The deceptive practices claim alleged that, since 2008, Wyndham had overstated its cybersecurity practices in its privacy policy. *See id.* at 241. "[C]ontrary to this policy, Wyndham did not use encryption, firewalls, or other commercially reasonable methods for protecting consumer data," according to the FTC. *See id.*

104. *See id.* at 259 ("We thus affirm the District Court's decision.").

105. *See id.* at 244–45 (explaining Wyndham's unsuccessful argument).

106. *See id.* (discussing prior cases that examined unfair conduct). Furthermore, Wyndham attempted to define an unfair practice as one that is "not equitable" or is "marked by injustice, partiality, or deception." *See id.* at 245. The Third Circuit reasoned that whether these are additional requirements was irrelevant in this case. *See id.* ("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.").

107. *See id.* at 244–47 (holding Wyndham's conduct does not fall outside of accepted notion of unfair practices).

108. *See id.* at 240, 242 (discussing consumer injury due to Wyndham's multiple breaches).

109. *See id.* at 241 ("We safeguard our [c]ustomers' personally identifiable information by using industry standard practices." (quoting Wyndham's advertised privacy policy)).

110. *See* Wyndham Worldwide Corporation, Annual Report (Form 10-K), SEC 35–36 (2013), http://www.sec.gov/Archives/edgar/data/1361658/000136165814000005/wyn-20131231x10k.htm [https://perma.cc/lb9e-5qdq] (disclosing Wyndham's total assets for fiscal year ending December 2013). Wyndham's total assets for the fiscal year ending December 31, 2013, were approximately $9.74 billion. *See id.* Its revenue topped $5 billion. *See id.*

111. *See Wyndham*, 799 F.3d at 252 (rejecting Wyndham's request for "ascertainable certainty" standard).

decided that "this case involve[d] ordinary judicial interpretation of a civil statute," the FTCA.[112] Therefore, the "ascertainable certainty" standard, which the Third Circuit applies only to an agency's interpretation of its organic statute or own regulations, was inapplicable.[113] The relevant question for the court was whether section 45(a) was so vague as to give Wyndham no expectation that its conduct *might* be a violation.[114] The court reasoned that "[f]air notice is satisfied here as long as [Wyndham] could reasonably foresee that a court *could* construe its conduct as falling within the meaning of the [FTCA]."[115] The court acknowledged that the three-part unfairness test is "far from" an exact standard but held that Wyndham was at least aware that it should have undertaken a cost-benefit analysis pursuant to the third requirement of the FTC's unfairness test.[116] According to the court, it should have been "painfully clear to Wyndham that a court could find that its conduct failed the cost-benefit analysis" in choosing not to respond to known threats after Wyndham's second data breach.[117] Furthermore, the court noted that the FTC's 2007 guidebook described a "checklist of [best] practices" for "sound data security plan[s]," which warns against many practices undertaken by Wyndham in this case.[118]

C. *Unfair Data Security Power in Beta: FTC & Consumers Win Because The Third Circuit Keeps Onus on Businesses to Adapt to New Threats*

The *Wyndham* holding is not the unfettered grant of unfair data security power that many claim it to be.[119] The Third Circuit's opinion, along with a comparison to the initial decision in *LabMD*, shows that the agency will be tethered to its three-part test for unfair practices in the future.[120] The court's

112. *See id.* at 253 ("[I]f the federal courts are to decide whether Wyndham's conduct was unfair in the first instance under the statute without deferring to any FTC interpretation, then this case involves ordinary judicial interpretation of a civil statute, and the ascertainable certainty standard does not apply.").

113. *See id.* (explaining when "ascertainable certainty" standard applies). This point was raised by Wyndham, as well, several times in the case. *See id.* Wyndham necessarily argued that the federal courts, rather than the agency, are to interpret section 45(a) in the first instance. *See id.* at 259.

114. *See id.* at 253–54 (explaining legal question).

115. *See id.* at 256 (emphasis added) (discussing considerations Wyndham should have been concerned with prior to breach).

116. *See id.* at 255 (citing Pa. Funeral Dirs. Ass'n v. FTC, 41 F.3d 81, 89–92 (3d Cir. 1994)) (stating Wyndham should have engaged in cost-benefit analysis of improved data security practices).

117. *See id.* at 256 (stating Wyndham had fair notice after second data breach).

118. *See id.* (noting Wyndham could have consulted FTC's guidebook).

119. *See* Brian Roux, *Understanding the Implications of* F.T.C. v. Wyndham *on Data Security Practices*, HANGARTNER RYDBERG & TERRELL LLC (Sept. 11, 2015), http://hanrylaw.com/2015/09/11/understanding-the-implications-of-ftc-v-wyndham-on-data-security-practices [https://perma.cc/235m-gh9s] (stating *Wyndham* stands for proposition that FTC already had data security authority under FTCA but might now be "unfettered by a company having made a deceptive promise").

120. *See Wyndham*, 799 F.3d at 243–44 (stating three-part test for unfairness and asserting not all consumer injuries lead to unfairness finding); *cf.* Initial Decision by D. Michael Chappell, Chief Admin. Law Judge, *In re* LabMD Inc., F.T.C. No. 9357, 2015 WL 7575033, at

determination that the "vagueness" standard applies, rather than the "ascertainable certainty" standard, is far more consequential and represents a positive outcome for consumers, as well as the FTC.[121]

1. *Comparing Older Models:* Wyndham *Compares Unfavorably to Previous Enforcement Actions*

The Third Circuit was able to avoid a discussion about how to regulate data security practices best because the facts were so overwhelmingly in the FTC's favor.[122] A comparison of *BJ's* and the initial decision from *LabMD* is instructive.[123] Given the quantifiable harm to consumers and glaring warning signs, *Wyndham* is much more like *BJ's* than *LabMD*.[124] Moreover, after several data breaches, Wyndham's data security practices presented more than a "mere risk" of consumer injury.[125] Wyndham's unfair data security practices caused actual consumer injury in the form of more than $10 million.[126]

2. *The Third Circuit Installs Vagueness Standard for FTC's Data Security Enforcement Actions*

The Third Circuit's application of the "vagueness" standard will enable the FTC to battle cyber threats effectively.[127] The opposite result would require the FTC to engage in notice and comment rulemaking before continuing unfair data security enforcement actions.[128] This process would be untenable because

---

*37 (F.T.C. Nov. 13, 2015) (citing Order Denying Respondent LabMD's Motion to Dismiss at 5, LabMD, F.T.C. No. 9357 (F.T.C. Jan. 16, 2014)) (refusing to revisit issue of FTC's jurisdiction in initial decision), *vacated*, F.T.C. No. 9357, 2016 WL 4128215 (F.T.C. July 28, 2016).

121. *See* Recent Cases, FTC v. Wyndham Worldwide Corp.*: Third Circuit Finds FTC Has Authority to Regulate Data Security and Company Had Fair Notice of Potential Liability*, 129 HARV. L. REV. 1120 (2016), http://harvardlawreview.org/2016/02/ftc-v-wyndham-worldwide-corp [https://perma.cc/gq4k-yu34] (arguing vagueness standard allows FTC to adapt to new data security threats).

122. *See id.* (noting facts that weighed against Wyndham and in favor of FTC).

123. *Compare* Initial Decision by D. Michael Chappell, Chief Admin. Law Judge, 2015 WL 7575033, at *37–38 (finding no evidence of anything more than "risk" posed by LabMD's data security practices), *with In re* BJ's Wholesale Club, Inc., 140 F.T.C. 465, 467 (2005) (noting consumers lost millions of dollars due to fraudulent charges).

124. *Compare Wyndham*, 799 F.3d at 240 (noting consumers lost $10.6 million in fraudulent charges), *with BJ's Wholesale Club*, 140 F.T.C. at 467 (noting fraudulent charges).

125. *Compare Wyndham*, 799 F.3d at 246 ("For good reason, Wyndham does not argue that the cybersecurity intrusions were unforeseeable. That would be particularly implausible as to the second and third attacks."), *with* Initial Decision by D. Michael Chappell, Chief Admin. Law Judge, 2015 WL 7575033, at *37–38 (finding no *actual* harm to consumers).

126. *See Wyndham*, 799 F.3d at 240 (noting consumers suffered $10.6 million in fraudulent charges).

127. *See* FTC v. Wyndham Worldwide Corp.*: Third Circuit Finds FTC Has Authority to Regulate Data Security and Company Had Fair Notice of Potential Liability*, *supra* note 121 (noting vagueness standard will allow FTC to adapt to new data security threats).

128. *See id.* (noting ascertainable certainty standard implies FTC would undertake rulemaking).

cybersecurity threats and business practices are constantly changing.[129] Specific compliance-based data security regulations would, in all likelihood, become obsolete shortly after passage.[130] Such a scenario would place no responsibility on businesses to improve their practices and would expose consumers' sensitive information to new modes of attack.[131] On the other hand, the FTC could promulgate data security regulations with the requisite flexibility, but they would be susceptible to the same fair notice challenges as the agency's current framework.[132]

As mentioned, this case presented an easy win for the FTC.[133] What would have happened if Wyndham had, on its own, made improvements to its data security practices after the initial breach, but stopped short of a comprehensive program due to its other operational interests?[134] Furthermore, what if the FTC disagreed with Wyndham's internal cost-benefit analysis in such a scenario?[135] Herein lies the tension created by the *Wyndham* holding: the FTCA and the FTC's guidance and enforcement actions give adequate notice to companies with egregiously unfair practices, like BJ's or Wyndham's, but not necessarily for companies with stringent, but not comprehensive measures.[136] A future court will

129. *See* Solove & Hartzog, *supra* note 11, at 624 (noting FTC's guidance on data security has been consistent).

130. *See* FTC v. Wyndham Worldwide Corp.*: Third Circuit Finds FTC Has Authority to Regulate Data Security and Company Had Fair Notice of Potential Liability*, *supra* note 121 (noting cybersecurity threats and business practices are always changing).

131. *See* Ira S. Rubinstein, *Regulating Privacy by Design*, 26 BERKELEY TECH. L.J. 1409, 1447 (2011) ("[The] combination of strategic enforcement and agency guidelines developed in collaboration with industry demonstrates the FTC's 'ability to respond to harmful outcomes by enforcing evolving standards of privacy protection' in keeping with changes in 'the market, technology, and consumer expectations.'" (quoting Bamberger & Mulligan, *supra* note 9, at 128–29)).

132. *See id.* at 1453 (discussing effects of flexible approach taken by FTC toward data security regulation); FTC v. Wyndham Worldwide Corp.*: Third Circuit Finds FTC Has Authority to Regulate Data Security and Company Had Fair Notice of Potential Liability*, *supra* note 121 (noting uniform privacy regulations would "necessarily be [] vague" and be open to same fair notice attacks as enforcement actions); *see also* Solove & Hartzog, *supra* note 11, at 625 (describing FTC approach as adaptable).

133. *See* FTC v. Wyndham Worldwide Corp.*: Third Circuit Finds FTC Has Authority to Regulate Data Security and Company Had Fair Notice of Potential Liability*, *supra* note 121 (noting facts in favor of FTC); Roux, *supra* note 119 ("[T]he alleged facts [were] so terribly against Wyndham."); Straight, *supra* note 76 (listing nine key data security practices that weighed against Wyndham).

134. *See* FTC v. Wyndham Worldwide Corp.*: Third Circuit Finds FTC Has Authority to Regulate Data Security and Company Had Fair Notice of Potential Liability*, *supra* note 121 (asking how future courts will rule in borderline cases); Roux, *supra* note 119 (noting implications of *Wyndham* are "not specific to companies of any particular size"); *see also* Straight, *supra* note 76 (stating companies must pay closer attention to data security practices).

135. *See* FTC v. Wyndham Worldwide Corp.*: Third Circuit Finds FTC Has Authority to Regulate Data Security and Company Had Fair Notice of Potential Liability*, *supra* note 121 (questioning how courts will rule under certain circumstances); Roux, *supra* note 119 ("The nuances of where the dividing line is for these issues were not discussed in this decision . . . .").

136. *See* FTC v. Wyndham Worldwide Corp.*: Third Circuit Finds FTC Has Authority to Regulate Data Security and Company Had Fair Notice of Potential Liability*, *supra* note 121 (asking how future courts will treat fair notice when company seemingly satisfies many data security practices requirements but still incurs FTC scrutiny); Edwards, *supra* note 20 (quoting

need to decide how the agency can enforce unfair data security practices while providing adequate notice to companies who are either financially unable to implement thorough practices or choose not to as a result of their own cost-benefit analyses.[137]

IV. THE THIRD CIRCUIT UPGRADES OBLIGATIONS: *WYNDHAM* HOLDING PUTS PRESSURE ON SMALL BUSINESSES IN NEW ERA OF "COMPLIANCE-PLUS"

Small to mid-sized companies are handling more and more sensitive information and often lack the resources they need to protect it.[138] The FTC has indicated that these companies will not "get a pass" when substantial consumer injury occurs.[139] This fact should set off alarms for businesses operating in the Third Circuit; "Losing [customers' confidence] due to a data breach" may mean life or death for a small business struggling to "keep[] the lights on."[140] The FTC's current posture suggests that small companies will be responsible for keeping pace with new forms of cyber threats, even when they are already doing what they can to secure personal information.[141] Thankfully, there are several steps smaller businesses and their legal counsel or compliance officers can take in pursuit of compliance with FTC data security standards.[142]

First and foremost, every company dealing with consumer information should incorporate data security into part of its technical and business strategy.[143]

Marc Roth, partner at Manatt, Phelps & Phillips, LLP) (noting that small companies may lack resources to comply with all of FTC's recommendations for data security programs).

137. *See* FTC v. Wyndham Worldwide Corp.*: Third Circuit Finds FTC Has Authority to Regulate Data Security and Company Had Fair Notice of Potential Liability*, *supra* note 121 (suggesting issue will need to be determined by future court).

138. *See* Julie Brill, Fed. Trade Comm'r, Keynote Address, *Do Try This at Home: Starting Up with Security*, FED. TRADE COMM'N (Feb. 9, 2016), https://www.ftc.gov/system/files/documents/public_statements/915043/160208swsseattle.pdf [https://perma.cc/2n5c-2vqf] (noting small businesses are collecting more and more sensitive information).

139. *See id.* ("Small companies can also get big very quickly. Neither new technologies nor small companies get a pass under the FTC Act."). The FTC's attitude should be cause for concern for smaller companies that do not have the resources to comply with the most stringent agency expectations. *See* Edwards, *supra* note 20 (quoting Marc Roth, partner at Manatt, Phelps & Phillips, LLP) ("For a small company, [compliance is] a challenge.").

140. *See* John Breyault, *Bravo! FTC's "Start with Security" Initiative Announces Seminar on Data Security*, NAT'L CONSUMERS LEAGUE (May 2015), http://www.nclnet.org/start_with_security [https://perma.cc/l5w3-lh9j] (noting approximately six out of ten consumers lose confidence in businesses after data breach).

141. *See* Edwards, *supra* note 20 ("If a company does what [it] can to protect data and gets hacked, should [it] have known that there's a new virus out there, or some type of intrusion device? It might be difficult for [it] to know that. But the FTC might bring a case." (quoting Marc Roth, partner at Manatt, Phelps & Phillips, LLP) (internal quotation marks omitted)).

142. *See* Sargent, *supra* note 39, at 542 (suggesting multiple "non-governmental sources" to use when discerning reasonableness of data security protocols).

143. *See* Mann et al., *supra* note 3, at 14 (noting importance of companies incorporating data security into business strategies). The authors argue that companies cannot leave I.T. professionals to deal with security problems on their own anymore. *See id.* In addition to having proper security networks, companies should implement "policies and practices that include[] training employees to identify [threats]." *See id.* at 15. Illustrative of this point is the

Businesses should start by undertaking a cost-benefit analysis, similar to the one discussed in *Wyndham*.[144] This analysis will entail evaluating the size and complexity of the company, the nature of the business, and the sensitivity of the information procured.[145] These determinations will vary by business, but programs such as those outlined by unfair data security enforcement settlements or the GLB will help weave data security into a company's strategic business plan.[146] Small businesses will not always be able to put in place such comprehensive programs, but might mitigate FTC scrutiny by doing so to the extent it is financially feasible.[147]

One thing all companies should do is consult the recommended security protocol developed by the National Institute of Standards and Technology.[148] This basic framework for cybersecurity "is becoming a de facto standard" for government regulation of data protection.[149] It pulls together data security developments in a variety of industries so that businesses do not have to.[150] The

2013 Target data breach. *See id.* The attack was just as much a result of an outside security vendor's own lack of a protection-minded "culture" as it was Target's "technical security failures." *See id.* at 13. Moreover, while I.T. professionals have a role to play in implementing such procedures, that role should be one part of a "culture of data security diligence." *See id.* at 14; Roux, *supra* note 119 ("It is clear that businesses must be proactive with their cybersecurity practices, forearm themselves with legally defensible procedures for dealing with the aftermath of an incident, and carefully consider their legal responsibilities . . . .").

144. *See* FTC v. Wyndham Worldwide Corp., 799 F.3d 236, 255 (3d Cir. 2015) (citing Pa. Funeral Dirs. Ass'n v. FTC, 41 F.3d 81, 89–92 (3d Cir. 1994)) (discussing flexible cost-benefit analysis that weighs consumer and business interests).

145. *See Cybersecurity and Consumer Data Hearing*, *supra* note 62, at 8 (noting key factors in crafting data security strategies); *cf. In re Dave & Buster's, Inc.*, 149 F.T.C. 1449 (2010) (outlining FTC investigation of Dave & Buster's and ordering changes to data security practices); *DSW Inc.*, F.T.C. No. C-4157, 2006 WL 752215 (F.T.C. Mar. 7, 2006).

146. *See* Pub. L. No. 106-102, § 501(b), 113 Stat. 1338, 1436–37 (1999) (codified at 15 U.S.C. § 6801(b) (2012)); *see also FTC Enforcement Actions*, *supra* note 10 (noting importance of making security part of business's service); *cf. Dave & Buster's, Inc.*, 149 F.T.C. 1449 (2010); *DSW Inc.*, F.T.C. No. C-4157, 2006 WL 752215 (F.T.C. Mar. 7, 2006).

147. *See* Richard Raysman & Francesca Morris, *What CIOs Need to Know About the FTC Cybersecurity Ruling*, W.S.J. (Aug. 31, 2015), http://blogs.wsj.com/cio/2015/08/31/what-cios-need-to-know-about-the-ftc-cybersecurity-ruling [https://perma.cc/xay3-fruj] (stating companies that attempt to implement cybersecurity framework may "persuade the FTC that there are no grounds to file a complaint").

148. *See id.* (claiming NIST framework will satisfy many FTC standards); *see also generally Framework for Improving Critical Infrastructure Cybersecurity*, NAT'L INST. OF STANDARDS & TECH. (Feb. 12, 2014), https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf [https://perma.cc/v8ly-5s88] (providing steps companies of every size can take to ensure compliance with FTC data security expectations).

149. *See* Raysman & Morris, *supra* note 147 (explaining framework "is becoming" government's preferred standard for cybersecurity).

150. *See Framework for Improving Critical Infrastructure Cybersecurity*, *supra* note 148, at 4 ("By relying on those global standards, guidelines, and practices developed, managed, and updated by industry, the tools and methods available to achieve the Framework outcomes will scale across borders, acknowledge the global nature of cybersecurity risks, and evolve with technological advances and business requirements.").

most recent update to the framework was made in 2014.[151] It accounts for a company's "risk tolerances[] and resources," while also considering what competitors in the industry are doing.[152] Using this protocol as a guide will show the FTC that an organization is attempting to keep pace with industry standards and respond to potential threats.[153]

V. CONCLUSION

While the standards for protecting consumer information appear to be amorphous, one thing is clear: documenting cybersecurity updates and attempts to keep pace with industry standards is of the utmost importance.[154] The ability to show that a company has made reasonable attempts at preventing breaches will go far to dissuade FTC enforcement.[155] Even the FTC concedes that no amount of spending will ensure complete data security.[156] However, providing evidence that a company has made data security a priority should help to mitigate FTC scrutiny.[157]

151. *See id.* at 2 ("The Framework . . . will continue to be updated and improved as industry provides feedback on implementation . . . . [L]essons learned will be integrated into future versions. This will ensure it is meeting the needs of critical infrastructure owners and operators in a dynamic and challenging environment of new threats, risks, and solutions."). In fact, the framework has already been updated since 2014, highlighting the pressure on businesses to keep pace with a rapidly evolving field. *See generally Framework for Improving Critical Infrastructure Cybersecurity*, NAT'L INST. OF STANDARDS & TECH., https://www.nist.gov/sites/default/files/documents/cyberframework/Cybersecurity-Framework-for-FCSM-Jan-2016.pdf [https://perma.cc/p8zl-ncgd].

152. *See Framework for Improving Critical Infrastructure Cybersecurity*, *supra* note 148, at 1, 4 (explaining continuous update to framework by industry).

153. *See* Raysman & Morris, *supra* note 147 (noting compliance efforts will possibly "dissuade the FTC from taking action").

154. *See id.* ("In addition to actually having in place the most up-to-date practical anti-hacking software, a company needs to be able to demonstrate the way in which it has protected private customer information in order to dissuade the FTC from taking action, and to protect its officers and directors . . . .").

155. *See id.* (suggesting companies may "dissuade" FTC from filing complaint by employing measures such as those suggested by NIST framework).

156. *See Cybersecurity and Consumer Data Hearing*, *supra* note 62, at 14 (stating companies with stringent data security practices may still suffer breaches).

157. *See* Raysman & Morris, *supra* note 147 ("[A] company needs to be able to demonstrate the way in which it has protected private customer information in order to dissuade the FTC from taking action, and to protect its officers and directors from class action lawsuits following an FTC complaint.").