DePaul Law Review

Volume 64
Issue 3 *Spring 2015: Twenty-Fourth Annual DePaul Law Review Symposium - Building the Solution: Connecting the Pieces of of Mental Health Law to Improve Mental Health Services*

Article 6

When a Data Breach Comes A-Knockin', the FTC Comes A-Blockin': Extending the FTC's Authority to Cover Data-Security Breaches

Amanda R. Moncada
amoncada2@gmail.com

WHEN A DATA BREACH COMES A-KNOCKIN', THE FTC COMES A-BLOCKIN': EXTENDING THE FTC'S AUTHORITY TO COVER DATA-SECURITY BREACHES

INTRODUCTION

Somewhere in the United States, an unsuspecting consumer is one credit card swipe away from being a victim of a data-security breach, exposing her financial or personal information to unauthorized third parties.[1] In 2007, this scenario was a reality for millions of consumers of the TJX Companies, Inc. (TJX), the "largest off-price department store chain in [America]," in what was once labeled the biggest data breach in history.[2] In 2013, however, Target Corporation (Target) surpassed TJX's record.[3] On December 19, 2013, Target informed the world that its United States stores experienced a massive data-security breach, compromising the personal and financial information of some 100 million customers.[4] As a result, Target sustained breach-related costs of $148 million.[5] Large data breaches affecting companies, such as TJX and Target, trigger a pivotal question for the United States government: who will ensure the protection of consumer data and privacy if not the companies with whom consumers willingly share their personal and financial information?

---

1. Abraham Shaw, Note, *Data Breach: From Notification to Prevention Using PCI DSS*, 43 COLUM. J.L. & SOC. PROBS. 517, 546 (2010); *see also* Complaint at 1, TJX Cos., No. C-4227, FTC File No. 072-3055 (July 29, 2008) [hereinafter *TJX* Complaint], 2008 WL 3150421.

2. Shaw, *supra* note 1, at 542, 545–46 (explaining that the TJX breach resulted in 94 million compromised credit cards because TJX scanned the credit card data from the magnetic strip of the cards and stored such information in clear, readable text, rather than using encryption); *see also TJX* Complaint, *supra* note 1, at 3.

3. *Neiman Marcus Falls Victim to Cyber-Security Attack, Says Some Customers' Cards Compromised*, TOLEDO BLADE (Jan. 11, 2014), http://www.toledoblade.com/Retail/2014/01/11/Neiman-Marcus-falls-victim-to-cyber-security-attack-says-some-customers-cards-compromised.html.

4. *Id.*; *see also A Message from CEO Gregg Steinhafel About Target's Payment Card Issues*, TARGET (Dec. 20, 2013), http://www.corporate.target.com/discover/article/Important-Notice-Unauthorized-access-to-payment-ca.; *Data Breach FAQ*, TARGET, http://www.corporate.target.com/about/shopping-experience/payment-card-issue-FAQ (last visited Feb. 4, 2014); Rachel Abrams, *Target Puts Data Breach Costs at $148 Million, and Forecasts Profit Drop*, N.Y. TIMES, Aug. 6, 2014, at B3, *available at* http://www.nytimes.com/2014/08/06/business/target-puts-data-breach-costs-at-148-million.html?_r=1.

5. Abrams, *supra* note 4, at B3.

As companies like Target increase their collection of consumer personally identifiable information (consumer PII), the inherent risks associated with data security and data privacy also increase.[6] Data breaches have become a worldwide epidemic.[7] Most breaches are the result of companies employing insufficient data-security practices, leaving consumer PII vulnerable to third-party exploitation.[8] This vulnerability in turn increases the threat to a consumer's physical and financial safety.[9]

In an effort to police the threat to consumer safety and data privacy, the Federal Trade Commission (FTC or Commission) has become the nation's primary enforcement agency.[10] It ensures that companies handling consumer PII implement reasonable data-security measures to protect such personal information.[11] The Commission pushes companies to self regulate by encouraging them to create custom security programs for their individual business models.[12] To assist companies

6. *See* Peter S. Frechette, Note, FTC v. LabMD*: FTC Jurisdiction over Information Privacy Is "Plausible," but How Far Can It Go?*, 62 AM. U. L. REV. 1401, 1401–02 (2013); VERIZON, 2012 DATA BREACH INVESTIGATIONS REPORT 2 (2012), *available at* http://www.verizonenterprise.com/resources/reports/pr_data-breach-investigations-report-2012-ebk_en_xg.pdf ("A study conducted by Verizon RISK Team with cooperation from the Australian Federal Police, Dutch National High Tech Crim Unit, Irish Reporting & Information Security Service, Police Central e-Crime Unit, and United States Secret Service.").

7. *See* VERIZON, *supra* note 6, at 2; *see also* Motion to Dismiss by Defendant Wyndham Hotels & Resorts LLC, FTC v. Wyndham Worldwide Corp., No. CV 12-1365 (D. Ariz. filed Aug. 27, 2012) [hereinafter *Wyndham* Motion to Dismiss], 2012 WL 3916987.

8. FTC v. LabMD, Inc., No. 1:12-cv-3005, slip op. at 14–15 (N.D. Ga. Nov. 26, 2012).

9. VERIZON, *supra* note 6, at 2*; see also Data Security and Security Breach Notification Act of 2010: Hearing on S. 3742 Before the Subcomm. on Consumer Prot., Prod. Safety & Ins. of S. Comm. on Commerce, Sci. & Transp.*, 111th Cong. 5 (2010) [hereinafter Sept. 22, 2010 FTC Statement] (prepared statement of Maneesha Mithal, Assoc. Dir. of the Div. of Privacy & Identity Prot., FTC).

10. Daniel J. Solove & Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, 114 COLUM. L. REV. 583, 604 (2014); *see also* Gerard M. Stegmaier & Wendell Bartnick, Essay, *Psychics, Russian Roulette, and Data Security: The FTC's Hidden Data-Security Requirements*, 20 GEO. MASON L. REV. 673, 674 (2013); *Discussion Draft of a Bill To Require Greater Protection for Sensitive Consumer Data and Timely Notification in Case of Breach: Hearing Before the Subcomm. on Commerce, Mfg. & Trade of the H. Comm. on Energy & Commerce*, 112th Cong. 43 (2011) [hereinafter June 15, 2011 FTC Statement] (prepared statement of Edith Ramirez, Comm'r, FTC).

11. Sept. 22, 2010 FTC Statement, *supra* note 9, at 5; *see also* June 15, 2011 FTC Statement, *supra* note 10, at 44.

12. *Balancing Privacy and Innovation: Does the President's Proposal Tip the Scale?: Hearing Before the Subcomm. on Commerce, Mfg. & Trade of the H. Comm. on Energy & Commerce*, 112th Cong. 40 (2012) [hereinafter Mar. 29, 2012 FTC Statement] (statement of Jon Leibowitz, Chairman, FTC), *available at* http://www.energycommerce.house.gov/sites/republicans.energycommerce.house.gov/files/Hearings/CMT/20120329/HHRG-112-IF17-WState-JLeibowitz-20120329.pdf; *see also* FTC, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE: RECOMMENDATIONS FOR BUSINESSES AND POLICYMAKERS, at i (2012) [hereinafter 2012 PRIVACY REPORT], *available at* http://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commis

in developing effective security programs, the Commission provides a de facto framework that can be derived from its practical guidelines, consent decrees, privacy reports, educational tools, and workshops.[13]

The Commission uses its statutory authority as the driving force behind its data privacy and security agenda.[14] Specifically, the Commission invokes Section 5 of the Federal Trade Commission Act of 1914 (FTC Act)[15] to monitor, investigate, and regulate a company's "deceptive" or "unfair" data-security practices.[16] To date, the Commission has used its Section 5 authority to bring over forty data-security lawsuits against companies for their failure to adequately protect consumer PII.[17]

A review of these lawsuits reveals that each FTC filing follows a similar process. First, the Commission investigates whether the company's data-collection practice violates Section 5.[18] After the investigation begins, the Commission may send a cease-and-desist order to the company regarding its data practice.[19] Next, the company and the Commission typically reach a settlement agreement memorialized in a consent decree.[20] The consent decree details the steps the company agrees to take to protect consumer data, such as completely refraining from a particular data-collection practice,[21] modifying a practice,[22] or

---

sion-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf.

13. 2012 PRIVACY REPORT, *supra* note 12, at 1, 22 (explaining that privacy by design involves a company building privacy into the development of its products or services); *see also* Mar. 29, 2012 FTC Statement, *supra* note 12, at 43–44; June 15, 2011 FTC Statement, *supra* note 10, at 50.

14. Frechette, *supra* note 6, at 1402; *see also* Stegmaier & Bartnick, *supra* note 10, at 674.

15. Federal Trade Commission Act of 1914 § 5, 15 U.S.C. § 45 (2012).

16. *Id.* § 45(a)(1); *see also* Frechette, *supra* note 6, at 1402; Herbert Hovenkamp, *The Federal Trade Commission and the Sherman Act*, 62 FLA. L. REV. 871, 871 (2010).

17. Edith Ramirez, Chairwoman, FTC, Keynote Address at the Technology Policy Institute Aspen Forum: The Privacy Challenges of Big Data: A View from the Lifeguard's Chair 2 (Aug. 19, 2013), *available at* http://www.ftc.gov/sites/default/files/documents/public_statements/privacy-challenges-big-data-view-lifeguard%E2%80%99s-chair/130819bigdataaspen.pdf; *see also* Plaintiff's Response in Opposition to Wyndham Hotels & Resorts' Motion to Dismiss at 2, FTC v. Wyndham Worldwide Corp., No. 2:12-cv-01365-PHX-PGR (D. Ariz. filed Oct 1, 2012) [hereinafter Plaintiff's Response], 2012 WL 4766957.

18. 15 U.S.C. § 45.

19. FTC v. Accusearch Inc., 570 F.3d 1187, 1193 (10th Cir. 2009).

20. *See, e.g.*, Agreement Containing Consent Order, EPIC Marketplace, Inc., No. C-4389, FTC File No. 112-3182 (Dec. 5, 2012) [hereinafter *Epic* Consent Decree], *available at* https://www.ftc.gov/sites/default/files/documents/cases/2012/12/121205epicorder.pdf.

21. *Id.* at 3.

22. Consent Decree & Order for Civil Penalties, Permanent Injunction & Other Relief at 12, United States v. Path, Inc., No. 3:13-cv-0048-RS (N.D. Cal. filed Feb. 8, 2013) [hereinafter *Path* Consent Decree], *available at* http://www.ftc.gov/sites/default/files/documents/cases/2013/02/130201pathincdo.pdf.

creating a better, more comprehensive security program altogether.[23] Finally, if a company violates the consent decree, the FTC may sue for civil penalties.[24] If, however, the company does not reach a settlement agreement, then the FTC may file a civil lawsuit against the company in federal district court, alleging an FTC Act violation.[25]

Investigating companies and drafting consent decrees is the standard protocol the Commission uses in its effort to prevent harm to consumer privacy in light of increased data breaches.[26] The decrees are made publicly available for other companies as they consider or reflect on their own data-collection practices.[27] In addition to the consent decrees, the Commission provides comprehensive guidelines detailing best practices to help companies develop reasonable data-security methods at the planning stages of their products or services.[28] The Commission also hosts workshops with interested stakeholders to discuss current data-security risks and to suggest proper ways to manage such risks.[29]

In response to its efforts, however, the Commission has been met with stark criticism about its data-security enforcement. Many opponents argue that the Commission lacks any authority whatsoever to regulate data security under Section 5,[30] because Congress has not explicitly confirmed the extent of such authority, if any, and the Commission has failed to create any formal rules to help enforce or

23. Decision & Order at 3, HTC America Inc., No. C-4406, FTC File No. 122-3049 (Feb. 22, 2013) [hereinafter *HTC* Consent Decree], *available at* http://www.ftc.gov/sites/default/files/documents/cases/2013/07/130702htcdo.pdf (describing that HTC Corporation agreed to develop a comprehensive security program and develop security patches to fix the security vulnerabilities of the pre-installation software that exposed consumer devices to malware); *see also Epic* Consent Decree, *supra* note 20, at 3 (establishing that Epic Marketplace will refrain from engaging in its "history sniffing" practice, which circumvented the consumer's ability to prevent online tracking).

24. 15 U.S.C. § 57(b).

25. *Id.* § 57(b)(1).

26. June 15, 2011 FTC Statement, *supra* note 10, at 44.

27. *See Legal Resources*, FTC BCP BUS. CENTER, http:// www.business.ftc.gov/legal-resources/all-35 (last visited Jan. 1, 2015).

28. FTC, FINAL REPORT OF THE FEDERAL TRADE COMMISSION ADVISORY COMMITTEE ON ONLINE ACCESS AND SECURITY (2000) [hereinafter 2000 PRIVACY REPORT], *available at* http://www.govinfo.library.unt/acoas/papers/acoasfinal1.pdf; *see also* FTC, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE: A PROPOSED FRAMEWORK FOR BUSINESSES AND POLICYMAKERS—PRELIMINARY FTC STAFF REPORT (2010) [hereinafter 2010 PRIVACY REPORT], *available at* http://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-bureau-consumer-protection-preliminary-ftc-staff-report-protecting-consumer/101201privacyreport.pdf; 2012 PRIVACY REPORT, *supra* note 12, at 1.

29. June 15, 2011 FTC Statement, *supra* note 10, at 51; *see also* Mar. 29, 2012 FTC Statement, *supra* note 12, at 52.

30. Stegmaier & Bartnick, *supra* note 10, at 691.

legitimize its assumed authority.[31] Some scholars, including law professor Gerard M. Stegmaier and attorney Wendell Bartnick, further argue that without federal action to limit the Commission's Section 5 authority, the Commission will continue to exceed the scope of Section 5 by overregulating data security, an area that does not explicitly fall under the unfair or deceptive categories of the FTC Act.[32]

In light of such criticisms, this Comment argues that Congress should amend the FTC Act to confirm the Commission's data-security authority under Section 5. Specifically, Congress should broaden Section 5 to state, "unfair or deceptive acts or practices in or affecting commerce[, *including any business or commercial practice that results in or has the potential to cause consumer injury*,] are hereby declared unlawful."[33] The flexible language of this amendment would provide the FTC the authority it needs to continue to regulate consumer data privacy using the data-security groundwork the Commission has already laid.

In anticipation of the fluid and quickly evolving technological marketplace, the Commission requires the flexibility to respond effectively without the hindrance of mandatory, formal rules which may prove obsolete over time,[34] or with the increased threat of opponents challenging the Commission's data-security authority in federal court. The Commission has already taken steps to create a de facto framework to guide a company's creation of effective data-security practices.[35] The Commission argues that it maintains an adequate amount of discretion in investigating and regulating the changing technological data marketplace.[36] This very marketplace is embracing more intimate practices of data collection and transferability, increasing public concern over consumer PII exploitation and data breaches.[37]

---

31. *Cf.* June 15, 2011 FTC Statement, *supra* note 10, at 53.

32. Frechette, *supra* note 6, at 1415; *see also* Michael D. Scott, *The FTC, the Unfairness Doctrine, and Data Security Breach Litigation: Has the Commission Gone Too Far?*, 60 ADMIN. L. REV. 127, 128–30 (2008); Stegmaier & Bartnick, *supra* note 10, at 676.

33. 15 U.S.C. § 45(a)(1) (2012) (bracketed text added).

34. *See* Frechette, *supra* note 6, at 1406; *see also* June 15, 2011 FTC Statement, *supra* note 10, at 53; Adam Thierer, *The Pursuit of Privacy in a World Where Information Control Is Failing*, 36 HARV. J.L. & PUB. POL'Y 409, 414 (2013).

35. *See* 2012 PRIVACY REPORT, *supra* note 12, at vii–viii (identifying best practices set by the FTC); Shaw, *supra* note 1, at 607 (noting a list of common inadequate data-security practices targeted by the FTC); *supra* notes 18–25 and accompanying text (detailing the process typically utilized by the FTC to establish consent decrees).

36. June 15, 2011 FTC Statement, *supra* note 10, at 53.

37. *See generally* Nancy J. King, *When Mobile Phones Are RFID-Equipped—Finding E.U.–U.S. Solutions To Protect Consumer Privacy and Facilitate Mobile Commerce*, 15 MICH. TELECOMM. & TECH. L. REV. 107 (2008); *FTC Seeks Input on Privacy and Security Implications of the Internet of Things*, FTC (Apr. 17, 2013), http://www.ftc.gov/news-events/press-releases/

Part II of this Comment discusses the Commission's use of the FTC Act in data-security cases. Specifically, Part II uses federal cases to demonstrate how the Commission currently regulates data-security practices under the "deceptive" and "unfair" prongs of Section 5.[38] Part III analyzes how the Commission has effectively handled data-security cases for years using its operative de facto framework, and explains that it should be granted Congress's legislative support to continue.[39] Part IV discusses how the Commission's current framework will continue to positively impact the future of data privacy and protect consumer and business interests alike in an advancing technological world.[40]

II. BACKGROUND

Section 5 of the FTC Act prohibits "unfair or deceptive acts or practices in or affecting commerce."[41] The authority to determine whether a practice is "deceptive" or "unfair" is granted to the Commission.[42] The Commission uses its Section 5 authority to bring data-security enforcement actions against companies it deems to have used deceptive or unfair practices in their collection or maintenance of consumer data.[43] These enforcement actions often result in a consent decree between companies and the Commission as part of a settlement.[44] A standard consent decree, depending on the nature of the security practice, requires that a company take several actions, including the (1) development of a comprehensive security program; (2) provision of biennial audits to the Commission regarding its compli-

2013/04/ftc-seeks-input-privacy-and-security-implications-internet-things; *Internet of Things—Privacy & Security in a Connected World*, FTC (Nov. 19, 2013, 8:30 AM), http://www.ftc.gov/news-events/events-calendar/2013/11/internet-things-privacy-security-connected-world.

38. *See infra* notes 41–119 and accompanying text.

39. *See infra* notes 121–257 and accompanying text.

40. *See infra* notes 258–278 and accompanying text.

41. 15 U.S.C. § 45(a)(1) (2012).

42. Orkin Exterminating Co. v. FTC, 849 F.2d 1354, 1363 (11th Cir. 1988).

43. Complaint at 7–8, HTC America Inc., No. C-4406, FTC File No. 122-3049 (June 25, 2013), *available at* http://www.ftc.gov/sites/default/files/documents/cases/2013/07/130702htccmpt.pdf; *see also* Complaint at 8–9, Facebook, Inc., No. C-4365, FTC File No. 092-3184 (July 27, 2012) [hereinafter *Facebook* Complaint], *available at* http://www.ftc.gov/sites/default/files/documents/cases/2012/08/120810facebookcmpt.pdf. The *Facebook* complaint explains that the Commission took action against Facebook, Inc. (Facebook) for its failure to adequately protect consumer privacy after launching its new privacy settings by subjecting consumers to the risk of "unwelcome contacts from persons who may have been able to infer their locale based on the locales of their Friends . . . and the organizations reflected in their Pages." *Facebook* Complaint, *supra*, at 8. The Commission established that this constitutes a deceptive practice because Facebook failed to disclose that consumers were no longer able to restrict access to their PII, including their names, picture, Friend List, and Networks. *Id.* at 8–9.

44. Frechette, *supra* note 6, at 1403.

ance with such program for twenty years; (3) provision of monetary redress to consumers and disgorgement of ill-gotten gains; (4) deletion of illegally obtained consumer information; and (5) provision of notice to those consumers who have been affected by the deceptive or unfair data practice.[45]

For example, the Commission brought an enforcement action against Path, Inc. (Path) for deceptive practices.[46] Path is a social networking service and an electronic journal application.[47] The Commission investigated Path in part due to Path's unauthorized collection of information from its consumers' mobile address book.[48] Pursuant to a consent decree, Path agreed to (1) develop a comprehensive privacy program, including development of physical safeguards to protect consumer PII; (2) disclose to consumers the categories of data Path collects; (3) obtain affirmative consent from consumers prior to collecting their data; and (4) provide the Commission an audit report detailing compliance with its newly created security program every two years.[49] This consent decree also provides the Commission the ongoing authority to monitor the company's commitment to consumer protection.[50]

A. Data-Security Enforcement Under the Deceptive Prong of the FTC Act

The FTC Act separates unlawful business practices into "deceptive" and "unfair" prongs, granting the Commission the authority to determine what conduct falls under which prong.[51] Though the FTC Act does not provide definitions for the terms "unfair" and "deceptive"[52] the Commission operates under judicially created tests to determine whether a practice is unfair[53] and deceptive.

To establish a claim for deception, the Commission must show that a company's business practice "is likely to mislead consumers acting

45. *Id.*; June 15, 2011 FTC Statement, *supra* note 10, at 46; *see also, e.g.*, *Path* Consent Decree, *supra* note 22, at 12–14. *See generally* FTC, 2014 PRIVACY & DATA SECURITY UPDATE (2014) [hereinafter 2014 PRIVACY UPDATE], *available at* http://www.ftc.gov/system/files/documents/reports/privacy-data-security-update-2014/privacydatasecurityupdate_2014.pdf.

46. Complaint at 9, United States v. Path, Inc., No. C-13-0448 (N.D. Cal. filed Jan. 31, 2013) [hereinafter *Path* Complaint], *available at* http://www.ftc.gov/sites/default/files/documents/cases/2013/02/130201pathinccmpt.pdf.

47. *Id.* at 3.

48. *Id.* at 4.

49. *Path* Consent Decree, *supra* note 22, at 12–14.

50. Frechette, *supra* note 6, at 1403.

51. 15 U.S.C. § 45(a)(1) (2012).

52. *See id.* § 44 (providing a list of definitions for Section 5 of the FTC Act).

53. *See infra* notes 73–75 and accompanying text for details regarding the "unfair" test.

reasonably under the circumstances."[54] The Commission typically invokes its deception authority in cases in which a company misrepresents or omits material information when representing or marketing its services or products.[55] The Commission has brought claims for deception against companies that have violated their own published privacy policy statements by either engaging in the unauthorized collection of data[56] or failing to uphold a promise to secure consumer data.[57]

For example, in 2011, the Commission brought a claim under the deceptive prong against Google, Inc. (Google) for violating its own published privacy policy.[58] In its policy, Google assured consumers that once they provided their personal information to sign up for any of its services such as Gmail, Google would request the consumer's consent prior to using the information in a manner different from the purpose for which it was initially collected.[59] But, after launching its social networking service "Google Buzz," Google automatically, and without prior notice or consumer consent, transferred its consumers' personal information from Gmail to Google Buzz.[60]

Consumers complained to Google that this automatic transfer of their personal data, in some instances, threatened exposure to unauthorized third parties such as abusive partners or parties against whom they had a restraining order.[61] As a result, the Commission took action against Google for breaking its own data-security promise.[62] In order to settle the action, Google and the Commission entered into a consent decree.[63] Under the decree, Google agreed to secure affirmative consent prior to sharing consumer information and to adequately disclose its data-collection practices in its policy statement.[64]

---

54. FTC v. Stefanchik, 559 F.3d 924, 928 (9th Cir. 2009).

55. *See, e.g.*, First Amended Complaint for Injunctive & Other Equitable Relief at 18, FTC v. Wyndham Worldwide Corp., No. 2:12-cv-01365-PHX-PGR (D. Ariz. filed Aug. 9, 2012) [hereinafter *Wyndham* Complaint].

56. *See, e.g.*, *Path* Complaint, *supra* note 39, at 8–9; Complaint at 5–6, Google, Inc., No. C-4336, FTC File No. 102-3136 (Oct. 13, 2011) [hereinafter *Google* Complaint], *available at* http://www.ftc.gov/sites/default/files/documents/cases/2011/10/111024googlebuzzcmpt.pdf.

57. *Wyndham* Complaint, *supra* note 55, at 18–19.

58. *Google* Complaint, *supra* note 56, at 2, 5–6.

59. *Id.* at 2.

60. *Id.* at 4.

61. *Id.* at 5.

62. Francoise Gilbert, FTC v. Google*: A Blueprint for Your Next Privacy Audit*, J. INTERNET L., Dec. 2012, at 1, 15.

63. Decision & Order, Google Inc., No. C-4336, FTC File No. 102-3136 (Oct. 13, 2011) [hereinafter *Google* Consent Decree], *available at* http://www.ftc.gov/sites/default/files/documents/cases/2011/10/111024googlebuzzdo.pdf.

64. *Id.* at 3–4.

The deceptive prong of the FTC Act holds companies accountable for the affirmative promises they make to consumers regarding their collection of consumer data.[65] Because these promises are affirmative misrepresentations, most companies do not push back against the Commission's enforcement of its deception authority.[66] Accordingly, companies must make every effort to ensure that they accurately represent their data-collection practices and policies to consumers.[67]

The Commission does, however, face pushback for its data-security enforcement actions brought under the unfair prong.[68] Companies generally argue that because the FTC Act does not explicitly grant the Commission authority over data-security matters, the Commission cannot regulate data-security breaches.[69]

B. Data-Security Enforcement Under the Unfair Prong of Section 5

The Commission often invokes its unfairness authority when companies fail to adequately protect the consumer PII they have collected.[70] Determining what is adequate is the major point of contention between the Commission and the companies it regulates.[71] The Commission's enforcement of data security under the second prong of Section 5 takes on a more demanding burden.[72] Under the unfair prong, the FTC Act requires the Commission to show that an unfair business practice "causes or is likely to cause substantial injury to consumers which is not reasonably avoidable by consumers themselves and is not outweighed by countervailing benefits to consumers or to competition."[73] Such a showing requires the Commission to pass a three-part test.[74] To meet the "substantial injury" requirement of

65. Frechette, *supra* note 6, at 1404; *see also* Gilbert, *supra* note 62, at 15; Ramirez, *supra* note 17, at 2 (explaining that the Commission is dedicated to making sure companies uphold their promises to keep data confidential).

66. Frechette, *supra* note 6, at 1404 ("The FTC has a relatively easy argument when it can show that a company has made promises to consumers that it has not kept.").

67. Gilbert, *supra* note 62, at 17.

68. *See, e.g.*, *infra* notes 101–102, 111–114, and accompanying text.

69. *Id.*

70. Frechette, *supra* note 6, at 1405.

71. *See, e.g.*, *Wyndham* Motion to Dismiss, *supra* note 7, at 21 (defendant company arguing that it did not engage in unfair practices because the data breach it sustained was caused by a third party that cost the company, not consumers, millions of dollars).

72. *See* Stegmaier & Bartnick, *supra* note 10, at 675 (contending that nothing in the FTC Act grants the Commission authority to regulate data security); *see also* Frechette, *supra* note 6, at 1406 (arguing that the Commission's authority under this prong is exceptionally broad); Scott, *supra* note 32, at 159 (arguing that absent legislative guidelines, the Commission's use of the unfairness doctrine will yield "an expansive and unwarranted use of the unfairness doctrine").

73. 15 U.S.C. § 45(n) (2012).

74. Solove & Hartzog, *supra* note 10, at 638.

this test, the Commission generally must show that the practice at issue has significant monetary, health, or safety risks for consumers.[75] The Commission typically brings a claim for unfair practices when companies fail to "employ reasonable security measures" that are likely to cause substantial consumer injury, including identity theft or fraudulent credit card transactions.[76]

Two classic and often-cited cases illustrating FTC action under the unfair prong are DSW, Inc. (DSW), a seller of men's and women's footwear,[77] and BJ's Wholesale Club (BJ's), a seller of food and general merchandise items.[78] Each company collected and stored consumer PII, including consumers' names and credit card or bank account information, on a wireless computer network.[79] BJ's and DSW transmitted unencrypted consumer information through their central computer networks.[80] As a result, consumers' credit and banking information was stolen and used for fraudulent purchases.[81] Under the unfair prong, the Commission took enforcement action against both companies, claiming failure to adequately protect consumer data through the use of reasonable data-security measures.[82]

When invoking its unfairness authority under Section 5, the question the Commission considers is not "what was promised" by the company, but "what was expected" of the company.[83] The Commission answers this question by establishing that the standard expectation is simply adequate data security.[84] According to the Commission, adequate security measures include creating administrative, technical, and physical safeguards to protect consumer data.[85] The depth and detail of these measures depend on the sensitivity of the data the company collects, the size and complexity of the company's data-collection operation, and the types of risks the company faces.[86] The larger the volume of and the more sensitive the consumer data that a com-

75. *Id.* at 639.

76. June 15, 2011 FTC Statement, *supra* note 10, at 44; *see also* FTC v. LabMD, Inc., No. 1:12-cv-3005, slip op. at 13 (N.D. Ga. Nov. 26, 2012); Scott, *supra* note 32, at 152; Stegmaier & Bartnick, *supra* note 10, at 674.

77. DSW Inc., 141 F.T.C. 117, 118 (2006).

78. BJ's Wholesale Club, Inc., 140 F.T.C. 465, 466 (2005).

79. *BJ's Wholesale*, 140 F.T.C. at 466–67; *DSW Inc.*, 141 F.T.C. at 118–19.

80. *BJ's Wholesale*, 140 F.T.C. at 467; *DSW Inc.*, 141 F.T.C. at 118–19.

81. *BJ's Wholesale*, 140 F.T.C. at 467; *DSW Inc.*, 141 F.T.C. at 119–20.

82. *BJ's Wholesale*, 140 F.T.C. at 467; *DSW Inc.*, 141 F.T.C. at 119–20.

83. Solove & Hartzog, *supra* note 10, at 667.

84. *Id.* at 662.

85. *BJ's Wholesale*, 140 F.T.C. at 472; *see also DSW Inc.*, 141 F.T.C. at 123.

86. *BJ's Wholesale*, 140 F.T.C. at 471; *see also DSW Inc.*, 141 F.T.C. at 123; June 15, 2011 FTC Statement, *supra* note 10, at 50.

pany collects, the more detailed and sophisticated the security measures should be, as there is a higher risk for unauthorized interception or potential consumer injury.[87]

C. Unfruitful Resistance to the Commission's Unfairness Authority in the Data-Security Context

The FTC has brought more than forty data-privacy lawsuits[88] and fifty cases alleging unfair and deceptive practices.[89] Two cases are of particular significance because they challenge the Commission's authority to regulate data security under Section 5: *FTC v. LabMD, Inc.*[90] and *FTC v. Wyndham Worldwide Corp.*[91] In each case, a company was the target of data-security breaches as a result of poor data-security practices.[92] The Commission brought claims against both companies alleging unreasonable data-security practices under the deceptive and unfair prongs of Section 5.[93] Though both companies argued that the Commission lacked authority to regulate data-security breaches,[94] their arguments have been met with skepticism by the courts.[95]

1. LabMD's Fight Against the FTC's Unfairness Authority

LabMD, Inc. (LabMD) is a company that conducts consumer clinical laboratory tests and reports the test results to the consumer's healthcare provider.[96] The Commission discovered that LabMD publicly disclosed the consumer PII of its nearly 9,300 consumers, including names, Social Security numbers, dates of birth, and personal health insurance information on its peer-to-peer (P2P) file-sharing network.[97] A common risk with P2P networks is that data can be

87. June 15, 2011 FTC Statement, *supra* note 10, at 50; *see also* Ramirez, *supra* note 17, at 6.

88. 2014 PRIVACY UPDATE, *supra* note 45, at 2.

89. *Id.* at 5.

90. No. 1:12-cv-3005, slip op. (N.D. Ga. Nov. 26, 2012).

91. 10 F. Supp. 3d 602 (D.N.J. 2014).

92. *LabMD*, No. 1:12-cv-3005, slip op. at 2; *Wyndham*, 10 F. Supp. 3d at 607.

93. *LabMD*, No. 1:12-cv-3005, slip op. at 1–2; *Wyndham*, 10 F. Supp. 3d at 607.

94. Petition to Limit or Quash the Civil Investigative Demand at 1, LabMD, Inc., No. 9357, FTC File No. 102-3099 (Jan. 10, 2012), *available at* http://www.ftc.gov/sites/default/files/documents/petitions-quash/labmd-inc./120110labmdpetition.pdf; *Wyndham* Motion to Dismiss, *supra* note 7, at 3.

95. *LabMD*, No. 1:12-cv-3005, slip op. at 8; *Wyndham*, 10 F. Supp. 3d at 612–15.

96. Complaint at 1, LabMD, Inc., No. 9357, FTC File No. 102-3099 (Aug. 28, 2013) [hereinafter *LabMD* Complaint], *available at* https://www.ftc.gov/sites/default/files/documents/cases/2013/08/130829labmdpart3.pdf.

97. *LabMD* Complaint, *supra* note 96, at 4; *see also* FTC, PEER-TO-PEER FILE SHARING: A GUIDE FOR BUSINESS 1 (2010) [hereinafter PEER-TO-PEER FILE SHARING], *available at* https://www.ftc.gov/system/files/documents/plain-language/bus46-peer-peer-file-sharing-guide-busi-

passed along to other P2P network users without downloading the file from the original source, making it nearly impossible to permanently erase data from the P2P network.[98] In this case, consumer PII was somehow made available to an unauthorized third party over LabMD's P2P network.[99] To determine whether this disclosure was the result of inadequate data-security practices in violation of the unfair prong of Section 5, and because such disclosure threatens substantial consumer injury, the Commission requested that LabMD turn over the files it held on its network.[100]

LabMD objected to the Commission's request, arguing that the Commission's use of the unfairness doctrine was improper because it does not have authority to regulate data security under Section 5.[101] The company further argued that the unfairness doctrine was improperly applied because the breach did not yield any substantial consumer injury.[102] The District Court for the Northern District of Georgia rejected both arguments, ruling that Section 5 "broadly confers authority on the FTC to investigate and regulate unfair practices."[103] Also, the court found that the *mere threat* of substantial consumer injury is sufficient to meet the consumer injury standard, allowing the Commission to investigate data-security matters, because issues such as identify theft are very common.[104] Through its rejection of LabMD's arguments and its statement that the Commission has broad Section 5 authority,[105] the court essentially confirmed the Commission's authority under Section 5 to regulate data security and consumer protection.

2. Wyndham's Fight Against the FTC's Unfairness Authority

In 2012, a legal challenge against the Commission came from Wyndham Worldwide Corp. (Wyndham), a hotel franchise, after it was hit with both deception and unfairness violations.[106] The Commission initiated an investigation of Wyndham for the company's failed privacy policy statement after it sustained three brute force attacks to its data-

---

ness.pdf (explaining that peer-to-peer file sharing is the transfer of data between two computers on a single online network).

98. *LabMD* Complaint, *supra* note 96, at 4.

99. *Id.*

100. *LabMD*, No. 1:12-cv-3005, slip op. at 2–4.

101. *Id.* at 11.

102. *Id.*

103. *Id.* at 8.

104. *Id.* at 12–13.

105. *Id.* at 8, 12–13.

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

security system within the span of eighteen months.[107] The Commission determined that these unsophisticated attacks were the result of Wyndham's security failures, which compromised over 600,000 payment card account numbers and over $10.6 million in fraudulent transactions.[108] The Commission argued that Wyndham was guilty of unfair business practices because it failed to employ simple security features such as firewalls, encrypted text for consumer PII, and complex passwords to make it difficult for hackers to access its security system.[109] Wyndham refused to enter into a consent decree, prompting the Commission to pursue legal action pursuant to Section 5 of the FTC Act in federal district court.[110]

Wyndham pushed back against the Commission, filing a motion to dismiss the Commission's legal action.[111] Wyndham asserted two major arguments. First, the Commission does not have data-security authority, especially because the company was a victim of third-party breaches.[112] Second, even if the Commission has such authority, the Commission must establish formal rules to enforce its authority.[113] Wyndham argued that Section 5 authority is routinely invoked to prevent companies from using "dishonest or unscrupulous business practices" that fall under the deceptive prong of Section 5 rather than the unfair prong.[114]

The district court heard the dispute, denying Wyndham's motion to dismiss and assuring both parties that the scope of the Commission's unfairness authority covers data breaches.[115] Specifically, the court's ruling in *Wyndham* is in harmony with the rulings of several other federal courts regarding the Commission's data-security authority.[116]

---

107. *Wyndham* Complaint, *supra* note 55, at 13 (explaining that a brute force attack is an unsophisticated attempt by a hacker to compromise a security system by repeatedly guessing the administrator's username and password, which leads to a system lockout because the hacker guessed incorrectly too many times).

108. *Id.* at 18.

109. *Id.* at 10–11.

110. *Wyndham*, 10 F. Supp. 3d at 616.

111. *Id.* at 607.

112. *Id.*; *see also* Motion to Dismiss by Defendant Wyndham Hotels & Resorts LLC at 21, *Wyndham*, 10 F. Supp. 3d 602 (No. 2:13-cv-01887-ES-SCM), 2013 WL 3475984 (stating that Wyndham, "unlike the consumers in this case, lost millions of dollars and suffered significant reputational harm when cybercriminals *attacked its network*").

113. *Wyndham*, 10 F. Supp. 3d at 607.

114. *Wyndham* Motion to Dismiss, *supra* note 7, at 2.

115. *Wyndham*, 10 F. Supp. 3d at 612.

116. *See, e.g.*, FTC v. Accusearch Inc., 570 F.3d 1187, 1195 (10th Cir. 2009) (stating that "the FTC may proceed against unfair practices even if those practices violate some other statute that the FTC lacks authority to administer"); FTC v. Ken Roberts Co., 276 F.3d 583, 586, 593 (D.C. Cir. 2001) (establishing the same); FTC v. LabMD, Inc., No. 1:12-cv-3005, slip op. at 8–9 (N.D. Ga. Nov. 26, 2012).

Several federal courts have established that, although not unlimited,[117] the Commission's authority is tailored broadly to confront "unprecedented situations."[118] Accordingly, the result of the district court's decision in *Wyndham* informs the remainder of the data-privacy world that the Commission's authority with respect to data-security matters is likely within the purview of the FTC Act.[119] Notwithstanding the court's decision in *Wyndham*, Congress has the power to, and should, confirm the scope of the Commission's data-security authority under Section 5 of the FTC Act so that there is no question regarding the Commission's authority.

III. Analysis

Congress should explicitly confirm the Commission's data-security authority and endorse the Commission's existing de facto framework. The best strategy Congress can employ is to amend the FTC Act to read "unfair or deceptive acts or practices in or affecting commerce[, *including any business or commercial practice that results in or has the potential to cause consumer injury*,] are hereby declared unlawful."[120]

This amendment to the FTC Act would grant the Commission explicit data-security authority and help the Commission maintain the liberty to adapt its enforcement practices appropriately in response to the evolving technological advances and data-collection methods employed by companies. The Commission's de facto framework is essentially "the closest thing the United States has to omnibus privacy regulation."[121] The Commission has been the only federal agency to regulate the data-security domain—a domain that would otherwise lack enforcement action, guidance, and protection.[122] Congress must acknowledge the effectiveness of the Commission's work and operate hand-in-hand with the agency to set a uniform national data-security standard.

An amendment to the FTC Act will help effectuate several goals the Commission has expressed concerning data security. First, the Commission's primary goal is to require companies to implement reasonable data-security practices due to the prevalence of data

117. *LabMD*, No. 1:12-cv-3005, slip op. at 10.

118. Orkin Exterminating Co. v. FTC, 849 F.2d 1354, 1368 (11th Cir. 1988) (quoting FTC v. Colgate-Palmolive, Co., 380 U.S. 374, 385 (1965)).

119. *See* Frechette, *supra* note 6, at 1414–15.

120. 15 U.S.C. § 45(a)(1) (2012) (bracketed text added).

121. Solove & Hartzog, *supra* note 10, at 676.

122. *Id.*

breaches.[123] Companies can, and should, expect the Commission to respond to insufficient data-security practices, especially given their "widespread impact and threat to consumers . . . that results from breaches of data security and consumer privacy."[124] Second, the Commission aims to work with companies to improve their technological innovations.[125] To effectuate this goal, the Commission encourages companies to regulate themselves by creating their own reasonable data-security models to match their individual needs, size, and complexity.[126] The Commission has provided several sources of guidance for companies to use in developing their security models, including privacy lawsuits,[127] consent decrees,[128] prepared statements,[129] consumer and business educational materials,[130] privacy reports, and workshops, town-hall meetings, and roundtables.[131]

The next Part of this Comment discusses (1) the existence and contours of the Commission's informal data-security authority; (2) the details of the Commission's de facto framework for data security; (3) the rising concerns with a constantly evolving technological marketplace; and (4) why the Commission's framework is ideal for the protection of consumer PII and technological innovations.

A. The Commission Has Informal Data-Security Authority

The development of the Commission's informal data-security authority begins with the 1972 Supreme Court ruling in *FTC v. Sperry & Hutchinson Co.*[132] In *Sperry*, the Court ruled against the Commission for its failure to show how Sperry & Hutchinson's conduct actually violated Section 5.[133] However, the Court made it clear that the construction of Section 5 authority should not be limited to govern only

123. Mar. 29, 2012 FTC Statement, *supra* note 12, at 1–3; *see also* June 15, 2011 FTC Statement, *supra* note 10, at 44; Sept. 22, 2010 FTC Statement, *supra* note 9, at 5.

124. FTC v. LabMD, Inc., No. 1:12-cv-3005, slip op. at 13 (N.D. Ga. Nov. 26, 2012).

125. *See* Mar. 29, 2012 FTC Statement, *supra* note 12, at 40–42.

126. *See* June 15, 2011 FTC Statement, *supra* note 10, at 50; *see also* Ramirez, *supra* note 17, at 4 (contending that "the FTC's role isn't [sic] to stand in the way of innovation; it is to ensure that these advances are accompanied by sufficiently rigorous privacy safeguards").

127. *See* 2014 PRIVACY UPDATE, *supra* note 45, at 2.

128. *See, e.g.*, *supra* notes 20, 22–23, and accompanying text.

129. *See supra* notes 9–10, 12, 28, and accompanying text.

130. *See, e.g.*, 2014 PRIVACY UPDATE, *supra* note 45, at 14.

131. *See* 2014 PRIVACY UPDATE, *supra* note 45, at 13.

132. 405 U.S. 233 (1972).

133. *Id.* at 234 (refusing to uphold the Commission's cease-and-desist order against Sperry & Hutchinson Co., a trading stamp company that allegedly violated Section 5 by unfairly regulating trading stamp exchanges, among other things).

unfair practices as it affects competing companies, but is read to also govern unfair practices as it affects consumers.[134]

Since the *Sperry* decision, the Commission has used its Section 5 authority to expand its reach to consumer data-security issues.[135] As the *Wyndham* case demonstrates, however, the scope of the Commission's self-imposed data-security authority is hotly debated.[136]

Although the language of Section 5 does not explicitly mention data-security or data-privacy matters, after over forty years of policing consumer privacy,[137] courts simply assume, and appropriately so, that such authority exists.[138] Since the Commission was established in 1914, Congress has not imposed strict limits on the Commission's authority because it "gave very broad powers to the FTC to protect consumers from deceptive and unfair trade practices."[139] Courts reason that a broad interpretation of the scope of the Commission's power is appropriate because creating a statute that enumerates all deceptive or unfair practices as they relate to Section 5 is an impractical task. This is especially true given evolving business practices and the need for relevant changes in the law to correspond to these practices.[140] Surely, after the Commission's inception, Congress anticipated a changing business climate and foresaw the need to have an equally evolving and responsive enforcement agency to address unforeseeable matters.[141]

Legal scholars, however, propose several arguments against the Commission's supposed data-security authority. First, several argue that the Commission may be inconsistent in its data-security-related advice to businesses because their data-security practices vary in type.[142] However, the Commission has been undeniably consistent in requiring companies to establish reasonable data-security practices to

---

134. *Id.* at 244 (reasoning that the FTC's authority reaches beyond antitrust matters and can be used to enforce actions or practices that are unfair to consumers).

135. 15 U.S.C. § 45(a)(1) (2012).

136. *See, e.g.*, *Wyndham* Motion to Dismiss, *supra* note 7; Scott, *supra* note 32, at 134–35; Kelsey Finch, FTC v. Wyndham*: Round One*, PRIVACY ADVISOR (Nov. 18, 2013), http://www.privacyassociation.org/publications/ftc_v._wyndham_round_one.

137. Mar. 29, 2012 FTC Statement, *supra* note 12, at 42; *see also* 2012 PRIVACY REPORT, *supra* note 12, at 1.

138. *See, e.g.*, FTC v. Accusearch Inc., 570 F.3d 1187 (10th Cir. 2009); Orkin Exterminating Co. v. FTC, 849 F.2d 1354 (8th Cir. 1988); FTC v. LabMD, Inc., No. 1:12-cv-3005, slip op. at 9–10 (N.D. Ga. Nov. 26, 2012).

139. Stegmaeir & Bartnik, *supra* note 10, at 687; *see also LabMD*, No. 1:12-cv-3005, slip op. at 8; *Orkin Exterminating*, 849 F.2d at 1368.

140. William E. Kovacic & Marc Winerman, *Competition Policy and the Application of Section 5 of the Federal Trade Commission Act*, 76 ANTITRUST L.J. 929, 930–31 (2010).

141. *See* Frechette, *supra* note 6, at 1413.

142. *E.g.,* Stegmaier & Bartnick, *supra* note 10, at 686.

offset consumer-privacy harm.[143] The *LabMD* court addressed this point quite clearly: "[P]oor data-security and consumer-privacy practices facilitate and contribute to predictable and substantial harm to consumers in violation of Section 5 because it is disturbingly commonplace for people to wrongfully exploit poor data-security and consumer-privacy practices to wrongfully acquire and exploit personal consumer information."[144] Unfair or deceptive practices that lead to consumer harm fall directly under the jurisdiction of the FTC Act.[145]

Second, critics argue that the Commission lacks data-security authority simply because the FTC Act does not include explicit language concerning data-privacy security.[146] This argument has clearly been met with skepticism by federal courts as recently as the *Wyndham* case.[147] Similarly, critics argue that the Commission's use of its unfairness authority to regulate data breaches is misplaced because hacking is often the result of third party intrusions whereby the company is merely a victim, lacking any intent to spark consumer injury.[148] The Commission's focus, however, is specifically on consumer injury, not "the mental state of the [company] accused of a [S]ection 5 violation"; therefore, a "party's intent has no bearing on the question of whether a [S]ection 5 violation has occurred."[149]

Finally, critics argue that in order to adequately inform companies on how best to avoid data-security enforcement actions, the Commission must provide formal rules and adjudications.[150] However, the FTC Act explicitly provides that the Commission "*may* prescribe . . . rules which define with specificity acts or practices which are unfair or deceptive," establishing that rule making is discretionary.[151] In fact, exercising this optional rule-making authority is such a burdensome

143. *Epic* Consent Decree, *supra* note 20, at 3; *Path* Consent Decree, *supra* note 22, at 12; *HTC* Consent Decree, *supra* note 22, at 3; *Google* Consent Decree, *supra* note 63, at 3.

144. FTC v. LabMD, Inc., No. 1:12-cv-3005, slip op. at 14 (N.D. Ga. Nov. 26, 2012); *see also* United States v. Mead Corp, 533 U.S. 218, 228 (2001) (establishing that courts grant deference to an agency after looking to the agency's consistency and the persuasiveness of the agency's position).

145. *See* 15 U.S.C. § 45(a)(4)(i) (2012) ("'[U]nfair or deceptive acts or practices' includes such acts . . . that cause or are likely to cause reasonably foreseeable injury.").

146. David J. Bender, Essay, *Tipping the Scales: Judicial Encouragement of a Legislative Answer to FTC Authority over Corporate Data-Security Practices*, 81 GEO. WASH. L. REV. 1665, 1677 (2013).

147. FTC v. Wyndham Worldwide Corp., 10 F. Supp. 3d 602, 613 (D.N.J. 2014) (holding that "the FTC's unfairness authority over data security can coexist with the existing data-security regulatory scheme").

148. Stegmaier & Bartnick, *supra* note 10, at 719–20.

149. Orkin Exterminating Co. v. FTC, 849 F.2d 1354 (8th Cir. 1988).

150. Stegmaier & Bartnick, *supra* note 10, at 693.

151. 15 U.S.C. § 57a(a)(1)(B) (2012) (emphasis added).

and time-consuming procedure that it would effectively render the Commission's authority useless because the Commission would have been too slow to respond to pressing issues at hand, such as frequent data breaches.[152] To illustrate the burden of the rule-making process, the Commission must (1) publish "a notice . . . [stating] with particularity the text of the [proposed] rule, including any alternatives";[153] (2) allow the opportunity for "interested persons to submit their written data, views, and arguments";[154] and (3) provide for an informal hearing where those interested persons can cross-examine each other.[155] The amount of time this process would require of the FTC is so onerous and ineffective "it is not surprising that the Commission has thus far not published any rules or regulations defining specific data-security policies."[156]

Aside from their procedural burden, formal rules are not always the most appropriate method by which federal agencies should regulate demanding and evolving issues.[157] In dynamic cases, problems must be remedied immediately, regardless of formal rules, and the federal agency must maintain the authority to deal with those issues "on a case-to-case basis if the administrative process is to be effective."[158] The data-collection arena is described as one of rapid technological change,[159] and the Commission cannot possibly anticipate all data-security issues in order to make applicable formal rules. As the Supreme Court stated, "Not every principle essential to the effective administration of a statute can or should be cast immediately into the mold of a general rule."[160]

As discussed above,[161] the authority to determine or construe what is deceptive or unfair under the FTC Act is granted to the Commission.[162] Accordingly, the FTC has broadened the scope of the deceptive and unfairness doctrines to include data-security matters plaguing today's society.[163] The Supreme Court, on more than one occasion,

152. Bender, *supra* note 146, at 1671; *see also* June 15, 2011 FTC Statement, *supra* note 10, at 53 (explaining that if the Commission is to develop rules, Congress must assist to help the Commission "promulgate these rules in a more timely and efficient manner").

153. 15 U.S.C. § 57a(b)(1).

154. *Id.*

155. *Id.* § 57a(c); *see also* Bender, *supra* note 146, at 1671.

156. Bender, *supra* note 146, at 1671.

157. SEC v. Chenery Corp., 332 U.S. 194, 202 (1947).

158. *Id.* at 203.

159. Thierer, *supra* note 34, at 414.

160. *Chenery*, 332 U.S. at 202.

161. *See supra* note 42 and accompanying text.

162. 15 U.S.C. § 45(a)(1) (2012).

163. June 15, 2011 FTC Statement, *supra* note 10, at 43.

has established that courts must defer to an agency's construction of the statute under which it operates, especially if Congress has failed to act or speak out regarding the specific legal issue.[164] Congress has yet to clearly act or speak regarding the Commission's inclusion of data-security matters under its Section 5 authority.[165] This silence is significant because data-security matters were not anticipated at the time Section 5 was enacted.[166] When Section 5 was drafted, the FTC Act was used exclusively to regulate unfair competition practices among companies,[167] but was expanded in 1972 by the Supreme Court to protect consumers from unfair trade practices.[168] Since 1999, the Commission has used its Section 5 authority to protect consumer PII collected and managed by companies, and to enforce against issues of inappropriate security practices.[169] The Commission's expansion of its Section 5 authority in these ways illustrates a flexible and evolving federal agency that adapts to the changing technological marketplace.

Furthermore, contrary to the argument about the Commission's possible inconsistency,[170] the Supreme Court has declared that an agency is not forced to commit to one particular interpretation of a statute.[171] The Commission notes that "its understanding of the unfairness doctrine is the result of an 'evolutionary process' that refines the standard over time through cases, rules, and . . . statements."[172] More importantly, even if the Commission has used different definitions for the term "unfair," doing so merely "adds force to the argument that the definition itself is flexible, particularly since Congress has never indicated any disapproval of a flexible reading of the statute."[173] And, if Congress has a change of heart concerning the Commission's authority, it "has not at any time withdrawn the broad discretionary authority originally granted the Commission."[174]

Consumer privacy is of such critical importance that limiting the Commission's authority to monitor data security would likely harm

---

164. Chevron U.S.A., Inc. v. Natural Res. Def. Council, Inc., 467 U.S. 837, 842–45 (1984); *see also* United States v. Mead Corp., 533 U.S. 218, 229 (2001).

165. Bender, *supra* note 146, at 1667.

166. *Id.* at 1681.

167. Kovacic & Winerman, *supra* note 140, at 930.

168. Bender, *supra* note 146, at 1668 (citing FTC v. Sperry & Hutchinson Co., 405 U.S. 233 (1972)); *see also* Kovacic & Winerman, *supra* note 140, at 937.

169. Shaw, *supra* note 1, at 538–39.

170. *See supra* note 142 and accompanying text.

171. Chevron U.S.A., Inc. v. Natural Res. Def. Council, Inc., 467 U.S. 837, 863 (1984) (reasoning that "[a]n initial agency interpretation is not instantly carved in stone").

172. Solove & Hartzog, *supra* note 10, at 638–39.

173. *Chevron*, 467 U.S. at 864.

174. Am. Fin. Servs. Ass'n v. FTC, 767 F.2d 957, 967 (D.C. Cir. 1985).

the American consumer. Simply put, if companies fail to implement reasonable data-security measures, as in the *Wyndham* and *LabMD* cases, consumers risk substantial harm, including fraud and threats to their physical safety.[175] The Commission serves as the strong arm of corporate accountability to ensure that companies reasonably protect consumer data, and its operative framework and evolving Section 5 authority provide both a detailed guideline for companies to use in developing their own data-security systems and a workable solution to calm consumer concerns.

B. The Commission Encourages a Flexible Self-Regulatory Framework

Part of the Commission's de facto framework serves to aid companies' attempt to self regulate their data-security practices. The framework includes notice and best practices.

1. The Commission Provides Notice and Guidance Regarding Its Deception and Unfairness Enforcement Methods

Companies, including Wyndham, and some legal scholars, argue that the Commission gives insufficient notice regarding its expectations in enforcing unfair practices.[176] Specifically, they argue that companies are not privy to the ways they can avoid a Section 5 enforcement action because the Commission has failed to issue formal rules or regulations before filing an unfairness claim.[177]

First, the FTC has the option of regulation by rule-making or by individual adjudication.[178] As established above,[179] the FTC does not "need to formally publish rules and regulations [because] the proscriptions in Section 5 are necessarily flexible."[180] Second, the Commission has provided a thorough bundle of information concerning data-security practices, including consent decrees, educational tools, workshops,

175. *See* FTC v. LabMD, Inc., No. 1:12-cv-3005, slip op. at 12–13 (N.D. Ga. Nov. 26, 2012); FTC v. Wyndham Worldwide Corp., 10 F. Supp. 3d 602, 607 (D.N.J. 2014); *see also* June 15, 2011 FTC Statement, *supra* note 10, at 43.

176. *Wyndham* Motion to Dismiss, *supra* note 7, at 11; Stegmaier & Bartnick, *supra* note 10, at 676.

177. Stegmaier & Bartnick, *supra* note 10, at 676, 691–92; *see also* Finch, *supra* note 136; *Wyndham* Motion to Dismiss, *supra* note 7, at 11.

178. 15 U.S.C. § 57a(a) (2012); *see also* PBW Stock Exch., Inc. v. SEC, 485 F.2d 718, 732 (3d Cir. 1973) ("The courts have consistently held that where an agency, as in this case, is given an option to proceed by rulemaking or by individual adjudication the choice is one that lies in the informed discretion of the administrative agency.").

179. *See supra* notes 150–151.

180. FTC v. Wyndham Worldwide Corp., 10 F. Supp. 3d 602, 619 (D.N.J. 2014).

and comprehensive guidelines on best practices.[181] Through its consent decrees, the Commission has given companies a blueprint which outlines its target areas in regard to enforcement of data-security and consumer-privacy issues.[182] Companies that engage in targeted behavior or activities that were once investigated by the Commission can likewise expect investigation from the Commission.[183] Specifically, the Commission has investigated companies for the following issues in terms of deficient data-security practices:

> (1) inadequately assessing system vulnerability to commonly known or reasonably foreseeable attacks; (2) failing to apply low-cost, simple, and readily available defenses; (3) using default user ID or passwords to protect sensitive data rather than stronger passwords to prevent hackers; (4) storing information in unencrypted files and sending sensitive data via unencrypted transmission routes; and (5) failing to develop unauthorized access detection mechanisms.[184]

The Commission's investigation of these particular practices is not surprising, because the Commission has made it explicitly clear that, at the very least, companies possessing consumer data should employ reasonable security measures to protect that consumer data.[185] As Professors Solove and Hartzog establish, employing adequate or reasonable security measures is the Commission's baseline standard, which has reverberated throughout the data world.[186] Surely, one can argue that companies that suffer a data breach are merely victims of criminal activity,[187] but many of these data-security issues are common threats that could be avoided simply by use of stronger administrative passwords or mechanisms that suspend logins after too many failed attempts.[188]

Some legal scholars, including Peter S. Frechette, contend that the Commission is drifting away from its self-regulatory approach by increased use of Section 5 enforcement actions and consent decrees,[189] but this could not be further from the truth. The Commission's en-

---

181. June 15, 2011 FTC Statement, *supra* note 10, at 43.

182. Gilbert, *supra* note 62, at 15–16; *see also* Shaw, *supra* note 1, at 542.

183. Solove & Hartzog, *supra* note 10, at 607.

184. Shaw, *supra* note 1, at 542.

185. *See, e.g.*, June 15, 2011 FTC Statement, *supra* note 10, at 44.

186. Solove & Hartzog, *supra* note 10, at 661.

187. Stegmaier & Bartnick, *supra* note 10, at 673.

188. *See* Sept. 22, 2010 FTC Statement, *supra* note 9, at 6 (explaining that the FTC brought an action against Twitter for its mere failure to require stronger passwords and its failure to suspend passwords after a number of login attempts, which enabled a hacker to gain control of the company's system by using a password-guessing tool).

189. Peter S. Frechette posits that the Commission is moving away from its self-regulatory framework because the agency "has become increasingly forceful in its use of [S]ection 5 to enforce information privacy and security." Frechette, *supra* note 6, at 1410–11

forcement process is more of an active compromise between the company and the agency.[190] The process begins with the Commission investigating the deceptive or unfair practice, a complaint to the company that provides for an opportunity to settle, and, if the company settles, the court issues a consent decree.[191] The consent decree is not an isolated judicial decision, but a "mutually agreed upon [settlement between] the FTC and the [company.]"[192] The consent decree is customized to fit the company's size and structure, similarly to how the company should have attempted to set its own security practices to fit its structure.[193] According to Solove and Hartzog, the decrees function much like a type of "privacy common law," which companies and their legal counsel can and should reference to gain an understanding of the pattern and predictability with which the Commission operates to enforce data security.[194] This is a direct response to the critical suggestion that the Commission might operate without any particular consistency in regulating data-security matters or without granting companies adequate enforcement notice.[195]

2. The Commission's Best Practices Guidelines Inform Companies on How To Implement Reasonable Security Measures

The Commission's involvement in regulating data security would certainly prove counterproductive if the agency failed to provide companies with guidelines on how to develop reasonable data-security practices, especially when increased business costs are at stake.[196] Accordingly, the Commission has developed a form of "soft law."[197] The Commission uses in-depth yet flexible privacy guidelines to assist companies in implementing reasonable data-security practices using three core technological principles: (1) privacy by design; (2) simplified consumer choice; and (3) greater transparency.[198] This framework, "while not controlling [on] the courts by reason of their

190. Solove & Hartzog, *supra* note 10, at 608–10 (labeling such process as "The Anatomy of an FTC Action").

191. *Id.* at 609–10.

192. *Id.* at 624.

193. *Id.* at 624–25.

194. *Id.* at 589–90, 608.

195. *See* Stegmaier & Bartnick, *supra* note 10, at 686.

196. *See id.* at 691 (explaining that the "penalties are serious and fair notice on how to avoid them seems warranted").

197. Solove & Hartzog, *supra* note 10, at 625.

198. 2012 PRIVACY REPORT, *supra* note 12, at vii–viii; *see also* Thierer, *supra* note 34, at 448 (discussing the FTC's "privacy by design efforts").

authority, do[es] constitute a body of experience and informed judgment."[199]

First, privacy by design requires companies to build consumer-privacy mechanisms into their products and services as they are being developed.[200] Companies should ask themselves, "Are [our] security measures appropriate given the volume and sensitivity of the data [we collect]?"[201] The security measures should include "physical, technical, and administrative safeguards."[202] Recall that these safeguards are included in the standard consent decrees issued by the Commission.[203] Additionally, companies should only collect consumer data that is necessary to accomplish their specific goals, and they should properly dispose of the data when it is no longer necessary.[204]

Second, simplified consumer choice requires that companies empower consumers with the tools necessary to "control whether their data is collected and how it is used," termed "choice mechanisms."[205] The choice mechanisms should be easy to use.[206] One common choice mechanism is the "do not track" feature, which allows consumers to opt out of having their data collected while online through the click of a button.[207] Google implemented a do not track mechanism for its search engine.[208] Use of these tools help promote a company's self-regulation.[209]

Third, transparency requires that companies make a better effort to inform consumers of their methods of collecting, using, and sharing consumer data.[210] Companies should provide this information in a "prominent, relevant, and easily accessible place at a time and in a context when it matters to [the consumer.]"[211] For example, mobile-service providers can develop standard graphic icons or other efficient

199. FTC v. Wyndham Worldwide Corp., 10 F. Supp. 3d 602, 621 (D.N.J. 2014) (quoting Gen. Elec. Co. v. Gilbert, 429 U.S. 125, 141–42 (1976)).

200. 2012 PRIVACY REPORT, *supra* note 12, at vii.

201. Ramirez, *supra* note 17, at 9.

202. June 15, 2011 FTC Statement, *supra* note 10, at 50.

203. *See supra* note 45 and accompanying text.

204. 2012 PRIVACY REPORT, *supra* note 12, at 26–28.

205. *Id.* at 35.

206. Ramirez, *supra* note 17, at 9.

207. 2012 PRIVACY REPORT, *supra* note 12, at 53.

208. Alex Howard, *FTC Calls on Congress To Enact Baseline Privacy Legislation and More Transparency of Data Brokers*, RADAR (Mar. 27, 2012), http://radar.oreilly.com/2012/03/ftc-calls-on-congress-to-enact.html.

209. *See* 2012 PRIVACY REPORT, *supra* note 12, at iii (stating that the Commission promotes self-regulation by calling for "improved privacy disclosures and choices," and internet organizations have responded by "developing a universal web protocol for Do Not Track").

210. *Id.* at 60.

211. *Id.*

ways to present quick, understandable policies to consumers regarding how the company will use their personal information.[212] Failure to comply with this principle is often the cause behind the enforcement actions brought by the Commission under the deceptive prong for unauthorized data-collection practices.[213] The overall goal is to make each company's privacy policy and data-collection method easy for consumers to access and to understand.[214]

These three principles allow companies to "implement the privacy protections . . . in a way that is proportional to the nature, sensitivity, and amount of data collected as well as the size of the business."[215] The focus on specialized security measures is key to helping each company develop its own reasonable security measures appropriate for its business type.[216] Implementing these guidelines to help companies engage in a self-regulatory method increases companies' willingness to innovate and compete for and increase benefits to consumers through the use of improved products and services.[217]

Significantly, the Obama Administration acknowledges that it is essential to build on the FTC's expertise.[218] The Administration also pushed for companies to develop adequate security standards to protect consumer data, provide understandable notice to consumers about their data-collection practices, and grant consumers control over what personal data is collected from them.[219] The Commission's framework has not only incentivized companies to improve their data-security practices, but it has also been flexible enough to encourage

212. *Id.* at 64; *see also* Michael Fertik, Comments of Reputation.com, Inc. (Jan. 28, 2011), *responding to* Notice of Inquiry: Information Privacy and Innovation in the Internet Economy, 65 Fed. Reg. 21226 (Apr. 23, 2010), *available at* http://www.ntia.doc.gov/files/ntia/comments/101214614-0614-01/attachments/Comments%20of%20Reputation.com%20Inc%20to%20the%20Department%20of%20Commerce-20110128.pdf.

213. *See supra* notes 47–49 and accompanying text.

214. Fertik, *supra* note 212, at 7.

215. *Id.* at 9.

216. *See* Dana Rosenfield & Donnelly McDowell, *Moving Target: Protecting Against Data Breaches Now and Down the Road*, ANTITRUST, Summer 2014, at 90, 93 ("There is no single 'correct' data-security plan as companies should adapt their policies and practices to the practical realities presented by their business model as well as the unique legal obligations affecting their industry and the type of customer information they collect and store.").

217. *See* 2012 PRIVACY REPORT, *supra* note 12, at 9 ("The privacy framework is designed to be flexible to permit and encourage innovation.").

218. *See* WHITE HOUSE, CONSUMER DATA PRIVACY IN A NETWORKED WORLD: A FRAMEWORK FOR PROTECTING PRIVACY AND PROMOTING INNOVATION IN THE GLOBAL DIGITAL ECONOMY 29 (2012) [hereinafter WHITE HOUSE REPORT], *available at* https://www.whitehouse.gov/sites/default/files/privacy-final.pdf.

219. *Id.* at 11, 14, 19.

companies to build and adapt privacy protections into their own products and services.[220]

However, as the Commission has recently noted, given this flexibility, companies have been slow to adopt adequate privacy protection.[221] Accordingly, the Commission has employed other practical avenues of assistance, including consumer education materials such as OnGuard Online,[222] a program that informs consumers about the risks of P2P file sharing and online threats such as spyware.[223] Articles providing tips on how to protect consumer PII while using features such as P2P file sharing are also available for businesses.[224]

Finally, the Commission has offered a seat at the table for all stakeholders, including businesses and consumers, to address data-privacy concerns through a series of workshops and roundtables.[225] Business representatives have acknowledged the importance of consumer trust in growing their companies.[226] Roundtables are essential to the area of privacy law because they improve the quality of advice on the substance and the process of developing an effective and evolving data-security framework.[227] All of the Commission's strategies taken together, including its consent decrees, best practices, online tools, roundtables, and workshops, serve to "illuminate the FTC's philosophy and approach, as well as its interpretation of [its] Section 5 [authority]."[228]

C. Technological Advancements and Increased Data Breaches Cause Consumer Privacy Concerns

America long ago bid farewell to the days when personal information traveled no further than an individual's geographic location.[229] As a result, data security is of increasing importance to consumers,[230] because information now travels the globe. "People want to know

220. 2012 PRIVACY REPORT, *supra* note 12, at 9.

221. 2010 PRIVACY REPORT, *supra* note 28, at 8.

222. ONGUARDONLINE, http://www.onguardonline.gov (last visited Jan. 1, 2015).

223. Mar. 29, 2012 FTC Statement, *supra* note 12, at 57.

224. *E.g.*, PEER-TO-PEER FILE SHARING, *supra* note 97.

225. *See Exploring Privacy: A Roundtable Series*, FTC, http://www.ftc.gov/news-events/events-calendar/2010/03/exploring-privacy-roundtable-series (last visited Nov. 14, 2013).

226. 2012 PRIVACY REPORT, *supra* note 12, at 8.

227. *See* WHITE HOUSE REPORT, *supra* note 218, at 23, 29.

228. Solove & Hartzog, *supra* note 10, at 626.

229. Thierer, *supra* note 34, at 426.

230. Sept. 22, 2010 FTC Statement, *supra* note 9, at 5.

they are safe."[231] This is especially true when businesses fail to adequately protect consumer data because of minor oversights that can cause private information to "fall into the wrong hands, resulting in fraud and other harm, and consumers [losing] confidence in the marketplace."[232] Data breaches are becoming more frequent. In 2011, at least 855 data breaches occurred worldwide, compromising over 174 million data records.[233] 97% of these breaches could have been avoided though the use of simple or intermediate countermeasures.[234] Many times, data breaches are the result of unsophisticated attacks to a company's data-security system, such as brute force attacks or a third party simply stealing the login credentials of an authorized employee.[235] The increased rate at which technology is evolving[236] only makes data privacy more of an alarming concern—one that should not be subject to unreasonable data practices or security measures.

Businesses and consumers participate in what is essentially an information marketplace.[237] For one, Americans are now transferring information online through multiple mediums, ranging from desktop computers to smartphones and other electronic devices.[238] Even the mobile phone has taken on sophisticated features whereby consumers can offer businesses their location information for navigation purposes, to obtain traffic updates, or to locate nearby stores.[239] To use these location-based services, consumers grant companies the right to locate and track their mobile phones, essentially determining the con-

231. John Hielscher, *Data Breaches Challenging Banks*, HERALD TRIB. (Feb. 9, 2014, 5:11 PM), http://www.heraldtribune.com/article/20140209/ARTICLE/140209664?p=1&tc=pg&tc=ar (quoting Don Martin, marketing director at Charlotte State Bank & Trust).

232. Sept. 22, 2010 FTC Statement, *supra* note 9, at 5.

233. VERIZON, *supra* note 6, at 2.

234. *Id.* at 3.

235. *See, e.g.*, FTC v. Wyndham Worldwide Corp., 10 F.3d 602, 624 (D.N.J. 2014); Michael Winter, *Home Depot Hackers Used Vendor Log-On To Steal Data, E-mails*, USA TODAY (Nov. 7, 2014, 8:57 AM), http://www.usatoday.com/story/money/business/2014/11/06/home-depot-hackers-stolen-data/18613167/. Home Depot's recent attack was the result of the hackers "obtaining an outside vendor's system credentials. The hackers often use targeted phishing emails to trick an employee into giving out credentials. Once they've entered the system through a compromised computer, the hackers install malware that gathers information from the computer and sends it back electronically to the hacker." Winter, *supra*; *see also* PONEMON INST., 2013 COST OF DATA BREACH STUDY: UNITED STATES 7 (2013), *available at* http://www.symantec.com/content/en/us/about/media/pdfs/b-cost-of-a-data-breach-us-report-2013.en-us.pdf (explaining that a high volume of data breaches were caused by criminal attack or mere employee negligence in 2012).

236. Thierer, *supra* note 34, at 414.

237. *See id*.

238. Pamela M. Prah, *Target's Data Breach Highlights State Role in Privacy*, USA TODAY (Jan. 16, 2014, 10:42 AM), http://www.usatoday.com/story/news/nation/2014/01/16/target-data-breach-states-privacy/4509749.

239. King, *supra* note 37, at 110.

sumer's physical location.[240] Accompanying this transfer of information is the inherent risk that the information will be exposed to or intercepted by unauthorized third parties, putting a consumer's safety at risk.[241]

The volume of information transferred and received through the Internet is exceptionally high. In fact, in 2007 alone, consumers worldwide transferred about 1.9 zettabytes of information online, which is as if every person on earth had received about 174 newspapers every day.[242] The transmission of personal data is so voluminous that the need for a framework for securing or policing such data is a problem without a one-size-fits-all solution.[243] However, consumer PII needs protection, and the Commission has been the driving force in this arena, "tak[ing] matters into its own hands by challenging inadequate corporate data-security practices . . . under [its] [S]ection 5 [authority]."[244] Congress must endorse the Commission's proactive efforts.

D. How Congress May Help the Commission Boost Data-Security Morale

The Commission's data-security regulation is effective and amenable. Indeed, the Commission has become the dominant regulatory force in the realm of data security and privacy.[245] Legislation should endorse the Commission's leadership, especially because Congress has not so much as raised a brow concerning the scope of the FTC's Section 5 authority since its inception.[246] Congress should amend Section 5 of the FTC Act's prohibition of unfair and deceptive practices to include any business or commercial practice that results in, or has the potential to cause, consumer injury. This modification will leave the Commission's framework and leadership as it has developed thus far untouched. This framework is most ideal for the current state of affairs related to data security.

Congress should proclaim it indisputable that the FTC has authority to regulate data-security matters, as the White House suggests.[247] The

240. *Id.* at 122.

241. *See id.* at 113.

242. Thierer, *supra* note 34, at 428.

243. *Cf. id.* at 433 ("When it comes to . . . information control efforts, there are not many good examples of fixes or silver-bullet solutions that have been effective, at least not for very long.").

244. Bender, *supra* note 146, at 1674.

245. Solove & Hartzog, *supra* note 10, at 605.

246. *See, e.g.*, Orkin Exterminating Co. v. FTC, 849 F.2d 1354, 1368 (11th Cir. 1988) (reasoning that Congress conferred broad authority to the Commission under Section 5).

247. WHITE HOUSE REPORT, *supra* note 218, at 36 (urging Congress to grant the FTC direct enforcement authority).

Commission has also advocated on its own behalf to have Congress draft legislation.[248] The Commission cautions, as have most scholars, that this legislation must be technologically neutral and flexible.[249] The best way to avoid overlegislating is to merely amend the FTC Act to expand the reach of unfair and deceptive practices to be more inclusive. This will ensure the neutrality and flexibility the data-security field needs.

As the Commission suggests, the security measures implemented by companies are dependent on the sensitivity of the data collected by the company, the size and complexity of the company's data collection, and the types of risks the company faces with such data.[250] Operating in an information marketplace, companies need the flexibility to innovate, not rigid rules that keep them and the Commission stagnant.[251] As one commentator suggests, "Today's solutions cannot anticipate all such future uses [of consumer information], and any solution must adapt to the rapid pace of technological changes."[252] Providing an amendment to the FTC Act will allow for a malleable and technologically evolving solution. The data-security world needs an enforcement agency that is in the business of data-breach prevention, not data-breach reaction.[253]

Though the Commission continues to regulate data-security matters, opponents increasingly challenge the existence of its authority to do so under Section 5, primarily because the FTC Act is void of any language regarding data-security matters.[254] Companies are starting to litigate in order to fiercely contest the Commission's power.[255] Their argument is simple: the FTC Act does not expressly state that the Commission has data-security authority, so the Commission cannot regulate data-security matters.[256] This argument makes Congress's silence on this issue increasingly problematic. Not only is the Commission urging Congress to act, but even Illinois Attorney Gen-

248. Mar. 29, 2012 FTC Statement, *supra* note 12, at 41; June 15, 2011 FTC Statement, *supra* note 10, at 52; Sept. 22, 2010 FTC Statement, *supra* note 9, at 8.

249. Mar. 29, 2012 FTC Statement, *supra* note 12, at 44.

250. June 15, 2011 FTC Statement, *supra* note 10, at 50.

251. Fertik, *supra* note 212, at 12.

252. *Id.*

253. Shaw, *supra* note 1, at 519.

254. *See supra* notes 30–31, 146, and accompanying text.

255. *See supra* notes 94, 106, 110–112, and accompanying text.

256. *See supra* notes 94, 101, 110–112, and accompanying text.

eral Lisa Madigan is "proposing that Congress give[ ] an existing federal agency the authority to investigate data breaches."[257]

An amendment to the FTC Act would easily facilitate this request and increase the Commission's ability to better protect consumers against data-security breaches because companies would undeniably be accountable to the Commission for inadequate data-security practices.

IV. IMPACT

A. The Effects of Endorsing the Commission's Working Framework

Section 5 of the FTC Act grants the Commission authority to define and regulate deceptive or unfair activities in the context of business practices.[258] Judicious use of Section 5 has made the Commission the country's largest consumer protection agency. With its Section 5 authority, the Commission has focused on one underlying standard in the context of data security: companies must develop reasonable data-security methods. The Commission's guiding principles—privacy by design, simplified consumer choice, and greater transparency—work to further this standard, and proves flexible and accommodating to businesses of all types and sizes. A flexible framework provides several positive effects for companies and consumers alike: (1) creative security and business models; (2) lower security costs; and (3) increased protection for consumers.

First, companies will likely experience an increased capacity to innovate, thereby increasing customer satisfaction and profits. Thierer said it best: "'Silver bullet' solutions won't work."[259] There is no one-size-fits-all data-security model that will work for all business types and data-collection models. Therefore, imposing a standard, which can be interpreted to benefit a company's individual needs, is the best approach. The development of creative solutions for data privacy will help spark competition because consumers will engage in business with companies which whom they feel safest.[260] Therefore, companies need the flexibility to generate creative solutions to fit their particular data-collection scheme. Companies, not government, are best suited

257. Sandra Guy, *Consumer Complaints About Data Breaches Skyrocket in Illinois*, CHI. SUN-TIMES.COM (Mar. 12, 2014, 6:29 AM), http://www.suntimes.com/news/metro/25512687-418/consumer-complaints-about-data-breaches-skyrocket-in-illinois.html.

258. *See* 15 U.S.C § 45(a) (2012).

259. Thierer, *supra* note 34, at 433.

260. WHITE HOUSE REPORT, *supra* note 218 ("Citizens who feel protected from misuse of their personal information feel free to engage in commerce . . . .").

to determine what is more appropriate for their individual business model.[261]

Second, improvements in data-security practices will also likely benefit companies and financial institutions by helping them to cut costs related to data breaches. Data breaches often result in fraudulent credit or debit card charges, leaving banks and credit unions to "eat the loss," or having companies suffer the loss, which can include drops in share values.[262] Financial institutions typically issue new cards to curb the onset of fraudulent transactions.[263] As a result of the Target breach, in particular, financial institutions reissued about 17.2 million debit and credit cards, costing about $172 million.[264] Similarly, companies sustain a comparable amount of financial loss due to data breaches. For example, the average organizational cost of major data breaches in 2012 was around $5.4 million.[265] These expenses include hiring forensic experts, credit monitoring, and investigations.[266] Adequate data-security methods will help offset the losses incurred by these financial institutions and decrease the threat of litigation by these institutions against companies that collect consumer data and suffer from data breaches. The Commission has already provided the blueprint for solving these issues—create reasonable data-security measures using privacy by design, consumer choice, and greater transparency.

Finally, consumers will receive stronger protection and increased privacy with respect to their personal data if businesses are required to prioritize and implement customized data-security measures in selling their products and services. Consumers are fearful of the consequences of data breaches. One consumer affected by the 2013 Target data breach commented that she became less confident about her fi-

261. For example, compare the data-security methods of Google and Microsoft Corp. (Microsoft). When Google launched its Google+ program, it used privacy as a structural component of the program's design, whereby users could *choose* with whom they wanted to share their information. Kashmir Hill, *Why "Privacy by Design" Is the New Corporate Hotness*, FORBES (July 28, 2011, 1:23 PM), http:www.forbes.com/sites/kashmirhill/2011/07/28/why-privacy-by-design-is-the-new-corporate-hotness (A Forbes Contributer blog). Conversely, Microsoft explains that its entire program is centered on the privacy by design concept, focusing on building privacy protections from the ground up. *Trustworthy Computing*, MICROSOFT, http://www.microsoft.com/en-us/twc/privacy/commitment.aspx (last visited Feb. 5, 2014).

262. Hielscher, *supra* note 231. Target suffered breach-related costs of around $148 million. Abrams, *supra* note 4, at B3.

263. Hielscher, *supra* note 231.

264. *Id.* These costs include producing new credit cards, informing consumers about the reissuance of the cards, activating the cards, and staffing call centers to handle consumer inquiries. *Id.*

265. PONEMON INST., *supra* note 235, at 1.

266. *Id.* at 3.

nancial safety while shopping at Target after the breach: "I was about to take out my credit card, and then I thought[,] . . . I'm not comfortable."[267] Consumer trust is in dire need of repair, and without it, companies will continue to suffer negative results.[268] The Commission's framework gives companies room to develop the best reasonable measures suited for their particular industry.

B. Why Congress's Amendment Matters for Consumers and Businesses Alike

Data-security breaches are effectively becoming commonplace in the technology market.[269] As a result, consumers are exposed to increased financial and safety risks.[270] A regulatory strategy must be developed to strike a healthy balance between consumer-privacy interests and companies' interest to innovate and derive profit. Data-security enforcement standards cannot be so rigid as to stifle business growth or give hackers time to exploit the rules.[271] Similarly, legislation should not be so lax as to give companies a license to push consumer privacy completely off their priority list.

The most effective balance is achieved through the Commission's framework and flexibility, which would be best provided through Congress's approval of a legislative amendment. A legislative amendment to the reach of unfair and deceptive practices provides three particular benefits: (1) it avoids any contradiction or conflict to existing FTC authority under the FTC Act while granting the Commission explicit authority to regulate data-security measures; (2) it avoids undermining the Commission's existing de facto data-security framework; and (3) it avoids hampering the creativity of businesses to generate sophisticated security models.

First, the FTC Act requires that the Commission regulate unfair and deceptive practices.[272] Under the Act, unfair and deceptive prac-

---

267. Beth Pinsker, *Consumers Vent Frustration and Anger at Target Data Breach*, REUTERS (Jan. 13, 2014, 7:28 PM), http://www.reuters.com/article/2014/01/14/us-target-consumers-idUSBREA0D01Z20140114.

268. *See* Abrams, *supra* note 4 ("It's going to take them a long time to build the trust of the shopper and get them to where they were prior to [its breach]." (quoting John Kindervag, vice president and principal analyst with Forrester Research)).

269. Paul Ziobro, *Target Data Breach Went on Longer than Thought*, WALL ST. J. (Feb. 4, 2014, 1:29 PM), http://www.wsj.com/articles/SB10001424052702304851104579362671467541380.

270. *See e.g.*, Kenneth R. Harney, *Retailers' Data Breaches May Damage Credit Scores of Home Buyers*, WASH. POST, Feb. 1, 2014, at EZ.3 (explaining that consumers whose credit card information is stolen can suffer damaging effects to their credit scores and credit reports, even if they are not liable for any fraudulent purchases).

271. Ziobro, *supra* note 269.

272. 15 U.S.C § 45(a).

tices include acts that "cause or are likely to cause reasonable or foreseeable injury" or involve material conduct.[273] To show an unfair practice, the Commission must satisfy a three-part test.[274] To show a deceptive practice, the Commission must show that the practice likely misled consumers.[275] Expanding the reach of unfair and deceptive practices to include "any business or commercial practice that results in or potentially causes consumer injury" does not tamper with the Commission's legal burdens under either the unfair or deceptive prongs. The addition would operate to unequivocally grant the Commission the authority to regulate data-security practices implemented by companies collecting consumer PII. This would eradicate the argument against the Commission's lack of data-security authority while making sure that the Commission is still bound by its statutory requirements. Therefore, courts can still apply the tests to show whether the Commission has met the applicable respective test for this broader scope of authority.

Second, an amendment to the FTC Act's reach of unfair and deceptive practices will work in tandem with and improve the potency of the Commission's existing de facto data-security framework. The Commission requires that companies provide reasonable data-security measures by employing privacy by design, consumer choice, and greater transparency.[276] Expanding the unfair and deceptive practices reach will provide increased incentive for companies to adhere to the Commission's standard. Similarly, it will reduce companies' power to push against the Commission's authority to regulate data security, as data-security practices would fall neatly into the "any business or commercial practice" part of the amended Act.

Finally, businesses often differ in their approaches to collecting and storing data, and the Commission should also differ in its approach to adequately monitor and regulate these businesses. Compare Google Wallet, a mobile application consumers can use to store and send money by sharing their own personal bank accounts,[277] to Pandora, a music streaming service that requires consumers to share their email address, birth year, gender, and zip code.[278] These applications use different personal data for different purposes. To be effective, the Commission must monitor them both to ensure consumer protection.

---

273. *Id.* § 45(a)(4)(A).

274. *See supra* notes 73–74 and accompanying text.

275. *See supra* note 54 and accompanying text.

276. 2012 PRIVACY REPORT, *supra* note 12, at vii–viii.

277. *Google Wallet*, GOOGLE, http://www.google.com/wallet/send-money (last visited Feb. 4, 2014).

278. *Privacy Policy*, PANDORA, http://www.pandora.com/privacy (last visited Feb. 4, 2014).

But there is no one-size-fits-all rule to place on each of these data-collection practices, nor is there one design method that will absolutely secure each data-collection practice. Because the Commission operates with a flexible standard, it can tailor its investigation and regulation strategies to fit the particular data practice under review. This means what the Commission and the respective company determines is an adequate or reasonable data-security practice for Google Wallet may differ entirely from that which is adequate for Pandora. Differences in regulation are necessary to push companies to engage in their best efforts in creating the ideal security programs to fit their company's size and data-collection methods.

Surely, the Commission's framework will not completely eradicate all data-security breaches, but a flexible enforcement agency backed by deferential data-security legislation will better equip the Commission to ensure that companies are doing their very best to guard against commonplace data-security risks. This type of strategy will help the Commission become an agency that engages in the prevention of data breaches, rather than one that merely reacts to a data breach.

V. CONCLUSION

Professors Solove and Hartzog's observation is a sound one: absent the Commission's already effective regulatory method, "the U.S. approach to privacy legislation would lose nearly all its legitimacy."[279] Consumers cannot afford to be left without protection at a time when personal data is easily transferrable and disposed of in the technological marketplace. Data breaches strike a mighty blow to consumer morale.[280] Breaches spark fear and distrust.[281] More business accountability is the answer.

The Commission has turned up the degree of Section 5 enforcement to an uncomfortable temperature, and companies are beginning to feel the heat. Target-like catastrophes are unacceptable to businesses and consumers alike. The Commission has proactively assumed the responsibility as the leading force behind consumer protection, and it has done an effective job thus far. If Congress plans to protect data privacy and consumer PII, it should start by acknowledging the FTC's

279. Solove & Hartzog, *supra* note 10, at 604.

280. Paul Ziobro & Danny Yadron, *Target Says Millions More at Risk*, WALL ST. J., Jan. 11–12, 2014, at B1 (positing that the data breaches experienced by Target and Neiman Marcus will "likely . . . heighten shoppers' concerns about the security of their personal and financial data").

281. *Id.*

data-security authority and endorsing the framework the FTC has already set in motion through a legislative amendment. Simply put, the Commission knows how to best address data-privacy concerns, and Congress should affirmatively acknowledge this fact to the rest of the data-privacy world.

*Amanda R. Moncada**

* J.D. Candidate, DePaul University College of Law, 2015; B.S., University of Illinois at Urbana-Champaign, 2010. I owe complete gratitude to the Volume 64 Editorial Board, my professors, and my attorney–mentors for all of their outstanding efforts in sculpting this article to its best form. I am exceptionally grateful to my father for his unmatched level of love and support, which encourages me to always pursue the depths of my dreams. Finally, to my youngest brothers, Mateo and Walter, thank you for inspiring me to be the best big sister the world has ever seen. Any errors are mine alone.