The Battle Against Breaches: A Call for Modernizing Federal Consumer Data Security Regulation

Alex Bossone *

TABLE OF CONTENTS

I. INTRODUCTION 228

II. THE CURRENT LEGAL FRAMEWORK FOR DATA SECURITY IS NEBULOUS – BUT THE THREAT OF BREACH IS VERY REAL 230

A. U.S. Federal Circuits Are Divided on an Individual Right of Action in the Event of a Breach 231

B. The FTC's Vague Role as the Unofficial U.S. Data Protection Agency 233

C. The FCC is Expanding its Role in Data Security Regulation, and is Taking a More Focused Approach Than the FTC 238

III. THE FTC SHOULD MOVE FORWARD WITH A SPECIFIC REQUIREMENTS ENFORCEMENT MODEL SIMILAR TO THE FCC'S APPROACH DEMONSTRATED IN COX 242

A. The FTC Needs to Provide Businesses with More Clarity on What Data Security Practices to Adopt, and When a Breach Should be Actionable 242

B. Data Breach Remedies Should Include Recourse for Consumers Commensurate with the Modern Value of Personal Data 245

IV. CONCLUSION 249

* J.D., The George Washington University Law School, May 2017. Senior Notes Editor, *Federal Communications Law Journal*, 2016–17.

I. INTRODUCTION

In the United States, the years 2013 and 2014 were marked by a series of high-profile data breaches that resulted in the theft of consumer payment information from various retailers' data systems. By May 2015, data breaches were on pace to cost roughly $70 billion annually[1] in the United States.[2] While not every consumer who had their personal information stolen incurred harm due to fraudulent charges or identity theft, many consumers have become wary of which companies they choose to do business with, and some have chosen to avoid using electronic payment methods that have been compromised by hacks.[3] Companies have also suffered losses as cyber-attacks have become increasingly frequent and costly.[4] The average data breach in 2015 cost $3.79 million for the victim company, eight percent more than the year prior, as negative publicity and expensive security measures take their toll on the bottom line.[5]

Consumers who are affected by breaches have turned to the courts for recourse, but federal circuit courts are split over when an individual may recover for a data breach claim. In *Remijas v. Neiman Marcus Group, LLC*, the United States Court of Appeals for the Seventh Circuit held that customers have Article III standing to seek relief against a company from which the customers' data was stolen, even where the data has not yet been harmfully used (for example, via fraudulent credit card charges).[6] In contrast, the Third Circuit held in *Reilly v. Ceridian Corporation* that data breach plaintiffs in a separate incident lacked Article III standing to recover where the alleged harm of an increased risk of identity theft from exposure of the data was deemed to be too hypothetical and incapable of being quantified.[7]

The circuit split highlights the inadequacy of available remedies for consumers in the event of a data breach, and the lack of a regulatory scheme that sufficiently reflects the increasing value of personal data. In contrast to many other countries that have specialized data privacy agencies (DPA) to administer a national regulatory framework for data privacy, the United States has designated the Federal Trade Commission (FTC) as its "de facto federal

1. This approximate number was reached by multiplying the per capita cost ($217) of domestic data breaches as of May, 2015 by the United States population as of January, 2015 (320 million). 2015 COST OF DATA BREACH STUDY: GLOBAL ANALYSIS 2, PONEMON INSTITUTE (2015), https://nhlearningsolutions.com/Portals/0/Documents/2015-Cost-of-Data-Breach-Study.PDF.

2. Bill Hardekopf, *The Big Data Breaches of 2014*, FORBES, (Jan. 13, 2015, 7:16 PM), http://www.forbes.com/sites/moneybuilder/2015/01/13/the-big-data-breaches-of-2014/#52151e823a48.

3. Brett Conradt, *Think Shoppers Forget Retail Data Breaches? Nope*, CNBC (June 22, 2015), http://www.cnbc.com/2015/06/22/think-shoppers-forget-retail-data-breaches-nope-commentary.html [https://perma.cc/EK5Y-Z2BX].

4. The average cost from lost business due to a breach was $1.57 million in 2015—up from $1.33 million the year prior. PONEMON INSTITUTE, *supra* note 1, at 2.

5. *Id.* at 1.

6. Remijas v. Neiman Marcus Grp., LLC, 794 F.3d 688, 693–95 (7th Cir. 2015).

7. Reilly v. Ceridian Corp., 664 F.3d 38 (3rd Cir. 2011).

DPA."[8] The FTC bases its data privacy authority on Section 5 of the FTC Act,[9] which establishes its power to guard against unfair or deceptive business practices. Other federal agencies claim narrower authority over the data practices of companies within their respective industries, with the Federal Communications Commission (FCC) pursuing enforcement actions over telecommunications and cable providers that suffer breaches.[10]

This Note will argue that Congress should augment the FTC's existing data security powers to preclude any challenges to the Commission's authority in that area, and to mandate a more effective framework by emulating the FCC Enforcement Bureau's approach. The Enforcement Bureau laid out its enforcement model in a 2015 data breach action that, for the first time, imposed specific technological requirements on a FCC licensee, in contrast to the FTC's approach of holding companies to a general "reasonableness" standard regarding data security practices.[11] The framework proposed in this Note would provide more specific guidelines to companies on how to keep their security practices up to date, and would provide incentives for businesses to follow the guidelines. The new regulations would also provide consumers with recourse in the event of a breach. As personal data becomes an increasingly valuable commodity, consumers face an unprecedented need for a reliable means of asserting their rights against the companies who profit from the use of data yet negligently handle it. As technology improves, data security systems will only become more complex, and hackers will only become more sophisticated. A new regulatory scheme addressing consumer data security requires specific solutions for businesses to ensure that data practices effectively keep pace with rapid technological developments and further integration of the Internet into individuals' daily lives. In addition, enforcement actions need to provide consumers with adequate remedies for the exposure of personal data, and should give businesses notice of the level of responsibility to which they will be held for failing to protect consumer data.

Accordingly, Part II of this Note will examine the circuit split over consumers' right of action in response to a breach, and will explore the FTC and FCC's roles in regulating the data security practices of U.S. businesses. Part III will discuss why the current regulatory framework for data security is insufficient to protect consumers from data breaches, and will outline what a new FTC regime of regulatory oversight based on the FCC's "specific

8. LEE A. BYGRAVE, DATA PRIVACY LAW: AN INTERNATIONAL PERSPECTIVE 177 (1st ed. 2014).

9. 15 U.S.C. § 45(a) (2015).

10. *See, e.g.*, Cox Commc'ns, Inc., 30 FCC Rcd 12302 (2015); Terracom, Inc., & Yourtel Am., Inc., 30 FCC Rcd 7075 (2015).

11. *See* Cox Commc'ns Inc., 30 FCC Rcd 12302, 12310 (2015); *see also FCC Expands Its Claim of Data Security Authority with Recent Enforcement Action Against Cox Communications*, ROPES & GRAY (Nov. 12, 2015), https://www.ropesgray.com/newsroom/alerts/2015/November/FCC-Expands-its-Claim-of-Data-Security-Authority-with-Recent-Enforcement-Action.aspx [https://perma.cc/WW8Y-753F]; *Cox Commc'ns*, 2015 WL 6779864.

requirements" enforcement method might look like. Finally, Part IV will offer conclusions and a brief summary of the proposed legislation.

II. THE CURRENT LEGAL FRAMEWORK FOR DATA SECURITY IS NEBULOUS – BUT THE THREAT OF BREACH IS VERY REAL

The prevailing U.S. policy approach regarding consumer data security at both the federal and state levels can largely be described as "hands-off," especially when compared with the protectionist approaches of countries in the European Union (EU).[12] Until 2003, when California passed the first state law requiring entities to notify individuals whose personal data have been compromised by a breach,[13] no government entity in the U.S. had undertaken broad legislative measures to protect data owners from third-party theft.[14] As for the establishment of a comprehensive regulatory scheme that covers both data privacy and protection, the EU has proved to be perhaps the most aggressive legislative body through its creation of the Data Protection Directive (DPD) in 1995.[15] The DPD, which is binding on all EU member states, establishes personal data protection as a "fundamental [human] right," and requires each EU member to create its own independent Data Protection Agency (DPA) to oversee and enforce domestic data security regulations.[16]

In contrast, the U.S. has designated the FTC as its own "de facto federal DPA," pursuant to the FTC's enforcement powers under Section 5 of the FTC Act regarding "unfair or deceptive business practices."[17] The FTC has also utilized a number of federal statutes related to the protection of very specific kinds of personal data.[18] Despite the FTC's recently expanded role in regulating data security practices, "its field of competence is more restricted than is typical for European DPAs."[19] One explanation for this divergence in policy approaches may be that U.S. corporations like Google and Facebook have lobbied for data legislation in the U.S. that EU authorities have viewed as insufficient to satisfy their own fundamentally held principle of data protection as a human right.[20] As the current data security paradigm stands in the U.S., the FTC has not been able to provide recourse for individual consumers who have had personal data stolen via increasingly costly retail

12. LOTHAR DETERMANN, DETERMANN'S FIELD GUIDE TO INTERNATIONAL DATA PRIVACY LAW COMPLIANCE xv (2012).

13. California's first attempt was contained in Cal. S.B. 1386, an amendment to Cal. Civ. Code § 1798.29.

14. *See* DETERMANN, *supra* note 12, at xiv ("[M]ost U.S. states and many countries [followed California's example]."); *see also* Getting it Right on Data Security and Breach Notification Legislation in the 114th Congress, (Hearing), 33 (2015).

15. DANIEL J. SOLOVE, INFORMATION PRIVACY LAW 53–54 (5th ed. 2015).

16. *Id.* at 59–60, 170.

17. *Id.* at 177–78.

18. *Id.* at 177–78; *see also* Fair Credit Reporting Act, 15 U.S.C. § 1641 (1970); Children's Online Privacy Protection Act, 15 U.S.C. §§ 6501–6506 (1998); Financial Services Modernization Act, Pub. L. 106–102 (1999).

19. SOLOVE, *supra* note 15, at 177.

20. *Id.* at 107.

data breaches, leaving them to fend for themselves in the courts – with varying measures of success.[21]

This section will first explore how courts have struggled to fully appreciate the harm that a data breach causes the affected consumers, especially in cases where the victims do not suffer immediate financial costs. Next, this section will discuss the FTC's vague "reasonableness" standard for commercial data security practices and will argue that the standard fails to adequately promote best practices among companies that handle consumer data. Finally, an examination of the FCC's more focused regulatory approach will follow, before moving on to a discussion of the proposed legislation.

A. U.S. Federal Circuits Are Divided on an Individual Right of Action in the Event of a Breach

The U.S. judicial system is ill suited to address the pressing need for a federal legal standard on consumer data security, as it lacks expertise and clear statutory guidance in that area. The split between the Third and Seventh Circuits is an example that some courts do not yet understand the increasingly high value of personal data and the harmful impact of breaches. [22] While many U.S. consumers have been left without a remedy for stolen personal data, the Seventh Circuit in *Remijas* recognized the cognizable harm that a retail data breach poses to the affected consumers, even where the precise level of financial harm cannot be calculated.[23] In 2014, a number of customers at Neiman Marcus brought a consolidated action against the retailer for a data breach that exposed approximately 350,000 credit card numbers, 9,200 of which were subsequently used to make fraudulent purchases.[24] Though the plaintiffs conceded that they were reimbursed by Neiman Marcus for the fraudulent charges, they argued successfully that they had incurred redressable harm in the form of: (1) mitigation expenses (the time and money lost resolving the stolen data issue and protecting themselves from future fraudulent charges or identity theft) and (2) future harm (the threat of potentially harmful uses of the stolen data at an unknown future time).[25]

In attempting to downplay the adverse impact of the breach on consumers, Neiman Marcus argued the Supreme Court's decision in *Clapper v. Amnesty International USA*[26] was controlling. The retailer contended that the plaintiffs did not have Article III standing to bring the future harm or mitigation cost claims because *Clapper* required that allegations of future harm be "'certainly impending' [to be deemed an injury-in-fact, while mere] 'allegations of possible future injury are not sufficient.'"[27] However, the

21. *See* Remijas v. Neiman Marcus Grp., LLC, 794 F.3d 688 (7th Cir. 2015*);* Reilly v. Ceridian Corp., 664 F.3d 38 (3rd Cir. 2011).

22. *Compare*, Clapper v. Amnesty International USA et al., 133 S. Ct. 1138 (2013), *with* Remijas v. Neiman Marcus Grp., LLC, 794 F.3d 688 (7th Cir. 2015), *and Reilly*, 664 F.3d 38.

23. *Remijas*, 794 F.3d at 693.

24. *Id.* at 690.

25. *Id.* at 692.

26. *See generally Clapper*, 133 S. Ct. 1138.

27. *Remijas*, 794 F.3d at 692 (citing *Clapper*, 133 S. Ct. at 1147).

Seventh Circuit found *Clapper* to be distinguishable from the case at hand because *Clapper* involved the *alleged* or *speculative* interception of communications data instead of the *actual*, *undisputed* theft of individual consumer data that occurred in *Remijas*.[28] Further, the court drew from *Clapper* a test for whether plaintiffs have standing to recover for future harm. In other words, there must be a "'substantial risk' that the harm will occur, which may prompt plaintiffs to reasonably incur costs to mitigate or avoid that harm."[29] Ultimately, the Seventh Circuit determined that the plaintiffs *did* face a "substantial risk" that some future harm would occur from the breach and therefore found that the plaintiffs had Article III standing.[30]

The *Remijas* holding represents a step in the right direction for the adjudication of data breaches, but there the Seventh Circuit did not quite demonstrate a full understanding of the concrete economic value that personal data holds. The Court correctly recognized that the harm caused by a breach does not only manifest itself in the actual, illicit use of the stolen data; instead, any breach or exposure of such data instantaneously results in a reasonably imminent loss of value for the individual victim.[31] As the court put it: "[w]hy else would hackers break into a store's database and steal consumers' private information" if that data did not hold any value to them?[32] However, the court narrowly interpreted that notion of personal data having an inherent value when the it declined to allow recovery for the breach as a "concrete injury" on the same level as theft of physical property.[33] Essentially, and somewhat paradoxically, the court seemed to reason that even though personal data can be used to financially benefit hackers at the victim's expense, that data does not grant the original owner any positive economic value that can be lost if the data is stolen.[34] Finally, the court reasoned that if potential data breach plaintiffs are forced to wait until fraudulent charges are made on their card or until their identity is stolen before bringing a claim, then the interim period of time would only leave more room (perhaps unjustifiably) for the defendant to argue that the plaintiff incurred harm due to a reason other than the breach.[35]

In its petition for *en banc* review to the Seventh Circuit, Neiman Marcus argued that there was a circuit split with regard to Article III standing, as evidenced by the Third Circuit's decision in *Reilly v. Ceridian Corporation*.[36] In Reilly, the court "held that an increased risk of identity theft from a payroll database breach doesn't satisfy Article III's injury-in-fact

28. *Id.* at 693 (emphasis added).
29. *Id.* (citing *Clapper*, 133 S. Ct. at 1150 n.5).
30. *See id.* at 693–4.
31. *See id.* at 694 ("[O]nce stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years." (quoting U.S. Gov't Accountability Office, GAO-07-737, report to Congressional Requesters: Personal Information 29 (2007))).
32. *Id.*at 693.
33. *Id.*at 695 ("Plaintiffs refer us to no authority that would support such a finding. We thus refrain from supporting standing on such an abstract injury, particularly since the complaint does not suggest that the plaintiffs could sell their personal information for value.").
34. *See id.* at 696.
35. *Id.*at 693; *see also* Adobe Sys., 66 F. Supp. 3d 1197, 2014 WL 4379916, at *8 n.5.
36. Reilly v. Ceridian Corp., 664 F.3d 38 (3d Cir. 2011).

requirements."[37] The Third Circuit then denied the appellants Article III standing on the following grounds:

> Appellants' contentions rely on speculation that the hacker: (1) read, copied, and understood their personal information; (2) intends to commit future criminal acts by misusing the information; and (3) is able to use such information to the detriment of Appellants by making unauthorized transactions in Appellants' names. Unless and until these conjectures come true, Appellants have not suffered any injury; there has been no misuse of the information, and thus, no harm.[38]

Though the facts in *Reilly* are different from in *Remijas* – *Reilly* involves purely speculative harm that might result from the breach while *Remijas* saw *some* actual harmful use of the exposed data (fraudulent charges on some of the cards) – the contrasting holdings reflect that the Seventh and Third Circuits disagree on one key point. As the Seventh Circuit pointed out in *Remijas*, the hackers would not have expended the effort to illegally access Neiman Marcus' data systems if not to derive some benefit or value from the personal data contained therein; thus, the potential for easily inflicted harm by the hacker(s) against the affected consumers was enough of an imminent threat to confer standing.[39] The Third Circuit in *Reilly* did not require a showing that the appellants' exposed data had been harmfully used to determine whether personal data has an inherent value; instead, the Court took a firm stance that there must be clear evidence the hacker physically looked at the exposed personal data (rather than merely accessing the system) for the harm to be sufficiently imminent.[40] The circuit split is evidence that courts, consumers, and data-collecting entities (retailers or otherwise) are all in need of some clarity regarding how the harm from a personal data breach should be legally assessed. Given the border-blurring nature of the Internet and the fact that hackers operate across state and national lines, an inconsistent approach among federal circuit courts on the issue of data breaches and the remedies provided to the individuals affected is no longer tolerable nor feasible.

B. The FTC's Vague Role as the Unofficial U.S. Data Protection Agency

The FTC holds the primary data security regulation and enforcement authority over U.S. companies, pursuant to its stated goal to prevent "deceptive" or "unfair" practices that are "in or affecting commerce" under

37. *See* Remijas v. Neiman Marcus Grp., 794 F.3d 688 (2015); *see also* Joey Godoy, *7th Circ. Won't Revisit Neiman Marcus Data Breach Ruling*, LAW360 (Sep. 17, 2015), http://www.law360.com/articles/704243/7th-circ-won-t-revisit-neiman-marcus-data-breach-ruling.

38. *Reilly*, 664 F.3d at 42.

39. *See Remijas*, 794 F.3d at 693.

40. *See Reilly*, 664 F.3d at 42.

Section 5 of the FTC Act.[41] Since 2002, the Commission "has brought more than 50 enforcement actions against companies that have engaged in unfair or deceptive practices that put consumers' personal data at unreasonable risk"– seven of those actions came in 2014 alone.[42] Some of these actions under the "deceptive" prong were taken against companies that were found to have misrepresented to consumers how the company plans to use their personal data,[43] while others were taken against companies that were found to have misrepresented the level of security of their data systems.[44] Some within the FTC claim that Section 5 is poorly suited for data security regulation, arguing that the "deceptive" acts authority unduly narrows the FTC's jurisdiction to instances where companies violate their own stated data security policies rather than where they violate a general legal standard.[45]

However, since the turn of the twenty-first century, the FTC has pursued a number of enforcement actions under its "unfair" acts authority under Section 5 that have supported a stronger – but still debated – claim to regulate the data security practices of companies generally.[46] For the data security actions that are broader in scope than those brought strictly under the "deceptive" prong of Section 5, a company's act is deemed "unfair" under a three-part test[47] if it "[(1)] causes or is likely to cause substantial injury to consumers [(2)] which is not reasonably avoidable by consumers themselves and [(3)] not outweighed by countervailing benefits to consumers or competition."[48] In addition to the FTC Act, more recent federal statutes such as the Fair Credit Reporting Act (FCRA), the Children's Online Privacy Protection Act (COPPA), and the Gramm-Leach-Bliley Act (GLBA) all grant the FTC affirmative data security authority in very specific areas – but this still means that in most industries, data security practices are only covered under Section 5's "deceptive" or "unfair" acts provisions.[49]

As far as the specific data security practices that companies are obligated to follow, the FTC has a flexible standard that requires businesses to undertake "reasonable" measures to keep consumer data secure.[50] This

41. 15 U.S.C. § 45(b) (2015).

42. FED. TRADE COMM'N, *2014 Privacy and Data Security Update* 5 (2014).

43. *See* FED. TRADE COMM'N, OFFICE OF PUB. AFF., *FTC Approves Final Order Setting Charges Against Snapchat* (Dec. 31, 2014).

44. *See FTC 2014 Privacy and Data Security Update* at 5.

45. Jeffrey Benner, *FTC Powerless to Protect Privacy*, WIRED (May 31, 2001), http://archive.wired.com/politics/security/news/2001/05/44173 (quoting Lee Peeler, former Associate Director of Advertising Practices at the FTC).

46. *See* FTC v. Wyndham Worldwide Corp., 10 F. Supp. 3d 602, 614–15 (D.N.J. 2014).

47. The Third Circuit was uncertain whether all three factors *must* be met to constitute an "unfair" act, or if they are instead merely sufficient conditions. *See* FTC v. Wyndham Worldwide Corp,, 799 F.3d 236, 244, 259 (3rd Cir. 2015).

48. 15 U.S.C. § 45(n) (2015).

49. Fair Credit Reporting Act, 15 U.S.C. § 1641 (1970) (regulating the use of consumer data by consumer reporting institutions); Children's Online Privacy Protection Act, 15 U.S.C. §§ 6501–6506 (1998) (regulating the use of data belonging to children under age thirteen); Gramm-Leach-Bliley Act, 15 U.S.C. § 6801(b) (regulating the use of consumer data in the hands of financial institutions); 15 U.S.C. § 45.

50. *See* Jessica Rich, Data Security: Why It's Important, What the FTC is Doing About It, FTC, 4 (Mar. 24, 2014), https://www.ftc.gov/system/files/documents/public_statements/295751/140324nclremarks.pdf, [https://perma.cc/KRE3-GSEQ].

"reasonableness" standard is grounded in the idea that "security is a continuous process of assessing and addressing risks; that there is no one-size-fits-all data security program; and that the mere fact that a breach occurs does not mean that a company has violated the law."[51] Factors that the FTC takes into account when making a reasonableness determination include "the sensitivity and volume of consumer information [the company] holds, the size and complexity of its business, and the cost of available tools to improve security and reduce vulnerabilities."[52] Although the FTC does provide some guidance on what constitutes reasonable data security practices, a bright-line rule that explicitly defines the "reasonableness" standard for companies to meet in order to avoid liability remains elusive.[53]

The FTC's interpretation of Section 5 as granting authority to regulate data security in commerce has not gone unchallenged.[54] In a recent data breach action against the Wyndham Worldwide hotel chain, the Third Circuit, on appeal from the United States District Court for the District of New Jersey, upheld the FTC's Section 5 authority over "unfair" data security practices after Wyndham claimed that such authority was an overextension of the FTC's congressionally granted powers.[55] *Wyndham* can be cited as a particularly egregious instance of a businesses' failure to take reasonable data security measures, as the company allowed hackers to steal hundreds of thousands of customers' personal and financial information over three separate instances, resulting in more than $10.6 million in fraudulent charges.[56] The FTC based its action on the ground that Wyndham did not take basic steps to protect its customers' data, and did not take preventative measures after the first breach, even though hackers used similar methods in the subsequent attacks.[57] When the FTC initially sued Wyndham in District Court, that court found Wyndham had committed a Section 5 "deceptive" acts violation by overstating its cybersecurity in a policy statement online.[58]

On appeal to the Third Circuit, Wyndham conceded the "deceptive" acts issue, but challenged the FTC's authority to bring a separate "unfairness" claim relating to the substance of the hotel chain's data security practices that led to the breaches.[59] Wyndham argued that Congress did not intend for Section 5 "unfair" act powers to grant the FTC any jurisdiction over data security, taking the position that the specific grants of data security jurisdiction under the FCRA, COPPA, and GLB would have been futile if the

51. *Id.*

52. *Commission Statement Marking the FTC's 50th Data Security Settlement*, FTC, 1 (Jan. 31, 2014), https://www.ftc.gov/system/files/documents/cases/140131gmrstatement.pdf, [https://perma.cc/P9NS-P6Y3].

53. *See generally Start with Security: Lessons Learned From FTC Cases*, FTC (Jun. 2015), https://www.ftc.gov/tips-advice/business-center/guidance/start-security-guide-business, [https://perma.cc/LF7T-DT2N].

54. *See* generally FTC v. Wyndham Worldwide Corp*.,* 799 F.3d 236 (3d. Cir. 2015).

55. *Id. See generally Start with Security: Lessons Learned From FTC Cases*

56. *See Id.* at 241-42.

57. *See Id.* at 241.

58. *See* FTC v. Wyndham Worldwide Corp., 10 F. Supp. 3d. 602, 626-28 (D.N.J. 2014).

59. *See* FTC v. Wyndham Worldwide Corp., 10 F. Supp. 3d. 602, 614 (D.N.J. 2014).

FTC had universal data security authority to begin with.[60] The Third Circuit rejected that argument on the ground that the newer acts *required*, rather than merely authorized, the FTC to regulate data security in their respective areas.[61] Furthermore, the statutes reduced some of the jurisdictional hurdles for the FTC to declare information security practices "unfair" in the covered industries, meaning that the newer statutes expanded, rather than proscribed, the FTC's existing data security authority under Section 5.[62]

The Third Circuit ultimately held that the FTC currently *does* have Section 5 authority over "unfair" data practices at least to some degree, but the ad hoc manner in which the Court interpreted the statutory application of "unfair" in regard to Wyndham's conduct provides little instructive value for future breach cases where businesses are not so plainly negligent.[63] The *Wyndham* holding thus illustrates a troublesome picture – both for the FTC, which lacks a solid legislative footing to define the legitimate scope of its data security jurisdiction, and for businesses that are left with hazy guidelines on how to grapple with cybersecurity.[64] There remains uncertainty as to how the three-part "unfair" acts test defines what data security measures are necessary in practice for a company to avoid an FTC action.[65] This ambiguity is especially apparent in more borderline breach cases where companies are not so plainly negligent, and cases where there has not been a "deceptive" misrepresentation by the company.[66]

In attempting to apply the three-part test, the Third Circuit problematically left open the possibility that the FTC's "unfair" acts authority is in fact entirely superfluous in the context of breaches. This suggests that the exceptionally narrow "deceptive" acts authority granted by Section 5 may provide the FTC's only vessel, however inoperable, for pioneering the uncharted jurisdictional void that data security presents.[67] The opinion did not conclude whether Section 5 required all three conditions to be met in order to declare an act "unfair," and the case was decided on the ground that Wyndham's conduct could not be shown to fall outside the ordinary meaning of "unfair."[68] The Court easily concluded that the breach exposed Wyndham's customers to the likelihood of substantial injury, as the first part of the Section 5 test requires.[69] For the second prong, which asks whether the injury was "reasonably avoidable by [the] consumers," the Court reasoned that Wyndham's misleading security policy plausibly could have prevented customers from avoiding the breach, and no alternative means of satisfying that inquiry were considered.[70] This is highly problematic as it suggests that a "deceptive" act may be *required* in order to meet the "unfair" act test for

60. *Id.* at 612–13.
61. *FTC v. Wyndham Worldwide Corp.*, 799 F.3d 236, 248 (3d Cir. 2015).
62. *Id.* at 248.
63. *See id.* at 258–59.
64. *See id.*
65. *See id.* at 258–59.
66. *See id.* at 245, 259 ("The three requirements in § 45(n) [(for unfair acts)] may be necessary rather than sufficient conditions of an unfair practice").
67. *See id.* at 245–46.
68. *See id.*
69. *Id.* at 245.
70. *Id.* at 245–46.

breaches, meaning the FTC's ostensibly broader "unfair" acts jurisdiction may be inseparable from the deception prong in consumer data breach cases. Unless there is conduct other than a company's *misrepresentation* that may satisfy the "reasonably avoidable" injury test, the FTC may be unable to use its "unfair" acts authority to pursue a data breach action outside the restrictive confines of its "deceptive" acts authority.[71]

While the second prong of the "unfair" acts test threatens to potentially narrow the scope of the FTC's jurisdiction, the third and final part further muddies the waters on a data security regulatory standard. The Court interpreted the third inquiry of whether the potential injury is "outweighed by countervailing benefits to consumers or to competition," as requiring a cost-benefit analysis between the heightened costs of various security measures as passed on to consumers and the risk of harm from breach.[72] This cost-benefit analysis was applied to examine Wyndham's security procedures in order to decide the merits of the hotel's separate claim that the FTC violated due process.[73] Wyndham contended that the FTC did not provide adequate notice as to what specific security measures are required to meet the "reasonableness" standard.[74] The Court, however, pointed to numerous FTC guidelines, publications and previous enforcement actions as providing a general idea of what data security measures a company can reasonably take, none of which Wyndham attempted to follow.[75] Though the Court found that Wyndham clearly failed to satisfy this third inquiry, it acknowledged that "there will be borderline cases where it is unclear if a particular company's conduct falls below the legal threshold," implying that companies may not have a precise means of determining what conduct the Third Circuit's cost-benefit analysis requires.[76] Essentially, the Court deferred to the FTC's "reasonableness" standard for company data practices, but it declined to explore the issue of whether or where a line for "reasonableness" can truly be drawn. Because the FTC has been left with the unwieldy Section 5 as its only statutory tool to craft a necessarily-sophisticated data security legal framework for all industries, concrete clarification of the "reasonableness" standard in *Wyndham* was forcibly set aside by the preliminary question of whether the FTC has data security authority in the first place. *Wyndham*, at a minimum, established that the FTC has jurisdiction over at least *some* companies that suffer breaches, but the holding should not give consumers much confidence that the FTC is currently in the position to elucidate and administer a regulatory regime that effectively safeguards personal data.

71. *See id.*
72. *Id.* at 255.
73. *Id.*
74. *Id.*
75. *Id.* at 256–57.
76. *Id.* at 256.

The FTC's heavy dependence on its decades-old authority to regulate "deceptive" or "unfair" practices as a jurisdictional hook[77] in data breach actions indicates that data security is thus far a legislative afterthought in the U.S., despite the reality that data security is a modern concern of paramount importance in all areas of commerce.[78] *Wyndham* demonstrates that although the FTC can assert a facially broad claim to regulate "unfair" data security practices, the one-size-fits-all nature of Section 5 may mean that for breaches, a "deceptive" act is required to satisfy the "unfair" act test.[79] This is problematic when compared with the Seventh Circuit's holding in *Remijas*, which arguably suggests that there is (or should be) an *implied* understanding that a company is undertaking adequate steps to protect consumer data in the course of business.[80] Thus, any *express* claims made by the company as to its proficiency in data security should be irrelevant. The FTC, in lacking an explicit grant of jurisdiction from Congress over data security, could be needlessly restricted only to pursuing companies that suffer data breaches *and* have explicitly misrepresented the security of their data systems.[81] Based on the somewhat contradictory opinions federal courts have handed down, it is evident that companies are in need of clearer guidance on how to properly secure their data systems, and that consumers could benefit from a more developed statutory framework.

C. The FCC is Expanding its Role in Data Security Regulation, and is Taking a More Focused Approach Than the FTC

Historically, the FCC has regulated the data security practices of telecommunications providers under interpretations of Sections 201(b), 222(a) and (c) of the Communications Act of 1934, in a manner that is similar to the FTC's "reasonable" practices standard.[82] Specifically, in a 2014 action against TerraCom and YourTel, two telecommunications companies who failed to protect the personal information of more than 300,000 customers, the FCC Enforcement Bureau reasoned that the language of Section 201(b), referring to "reasonable" practices, created an enforceable duty to protect

77. *See, e.g.*, Credit Karma, Inc., No. C-4480 (F.T.C. Aug. 13, 2014) (consent order), available at https://perma.cc/G5RM-M2UMhttp://www.ftc.gov/enforcement/cases-proceedings/132-3091/credit-karma-inc; Fandango, LLC, No. C-4481 (F.T.C. Aug. 13, 2014) (consent order), available at https://perma.cc/W65Y-BVPRhttp://www.ftc.gov/enforcement/cases-proceedings/132-3089/fandango-llc; TRENDnet, Inc., No. C-4426 (F.T.C. Jan. 16, 2014) (consent order), available at https://perma.cc/F4RL-Q4GUhttp://www.ftc.gov/enforcement/cases-proceedings/122-3090/trendnet-inc-matter.

78. *Discussion Draft of H.R.__, Data Security and Breach Notification Act of 2015: Hearing Before the H. Comm. on Energy & Commerce, Subcomm. On Commerce, Mfg., & Trade*, 114th Cong. 1–2 (2014) (statement of Jessica Rich, Dir. Bureau of Consumer Prot. at the FTC).

79. *See* FTC v. Wyndham Worldwide Corp., 799 F.3d 236, 245–46 (3d Cir. 2015).

80. *See* Remijas v. Neiman Marcus Grp., LLC, 794 F.3d 688 (7th Cir. 2015).

81. 15 U.S.C. § 41 (2012).

82. 47 U.S.C. §§ 201(b), 222(a), (c) (2012); *see also* Terracom, Inc., & Yourtel Am., Inc., *order*, 30 FCC Rcd 7075 (2015).

such personal data from unauthorized access or use.[83] Section 222(a) affirmatively imposes a duty on telecommunications providers "to protect the confidentiality of proprietary information [(PI)] of, and relating to … customers,"[84] while Section 222(c) limits the use of customer proprietary network information (CPNI) collected incidentally during the provision of telecommunications services to reasonable uses.[85] All enforcement actions taken by the FCC, pursuant to Sections 201(b) and 222(a) and (c), against telecommunications providers have involved incidents where customers' information was either accessed unlawfully by company personnel or was placed in a publicly accessible folder on the Internet.[86]

In 2015, the FCC sought to expand its data security regulatory authority to cable providers by pursuing a data breach action against Cox Communications.[87] The FCC Enforcement Bureau utilized Section 631 of the Communications Act, which regulates cable providers, to issue an order and consent decree after Cox lost its customers' personal information in a breach.[88] The relevant portion of Section 631(c) provides that a cable operator:

> [S]hall not disclose personally identifiable information concerning any subscriber without the prior written or electronic consent of the subscriber concerned and shall take such actions as are necessary to prevent unauthorized access to such information by a person other than the subscriber or cable operator.[89]

Since Cox is a provider of broadband and telecommunications services, in addition to cable, the Enforcement Bureau additionally determined that Sections 201 and 222 of the Communications Act also should apply.[90]

The primary focus of the Enforcement Bureau's order was to prevent further security lapses of the specific type that Cox suffered in the present instance.[91] The breach involved a hacker pretending to be a Cox employee, who then convinced a legitimate employee of the telecommunications provider to enter her internal account ID and password into a fake website controlled by the hacker, an activity known as "phishing," who then was able to access Cox's data systems.[92] According to the Enforcement Bureau, "at the time of the breach, Cox employed multi-factor authentication for some

83. 47 U.S.C. § 201(b) (2012) ("[a]ll charges, practices, classifications, and regulations for and in connection with [[interstate or foreign] communication service [by wire or radio], shall be just and reasonable, and any such charge, practice, classification, or regulation that is unjust or unreasonable is declared to be unlawful").
84. 47 U.S.C. § 222(a) (2012).
85. 47 U.S.C. § 222(c) (2012).
86. *See, e.g.,* Terracom, Inc., & Yourtel Am., Inc., *order*, 30 FCC Rcd 7075, 7081 (2015).
87. *See* Cox Commc'ns, Inc., *order*, 30 FCC Rcd 12302 (2015).
88. *See id.* at 12307; *see also* ROPES & GRAY, *supra* note 11.
89. 47 U.S.C.A. § 551(c)(1) (2012).
90. Cox, 30 FCC Rcd at 12307–08.
91. *Id*. at 12304.
92. *Id.* at 12308.

employees and third party contractors with access to Cox electronic data systems, but not for the compromised employee or contractor."[93] As a result, one of the specific requirements that the Enforcement Bureau imposed on Cox was to implement a standard system whereby the company takes targeted steps to ensure the security and authenticity of communications among Cox employees and third parties contractors.[94]

The FCC's pursuit of a breach action against a cable provider was a novel practice for the agency, but the biggest departure from its previous actions was the uniquely tailored remedy the agency sought to enforce on Cox. In lieu of ordering Cox to comply with the general "reasonable" practices standard, the Enforcement Bureau proposed a number of specific requirements as part of an overall "compliance plan."[95] Included in the compliance plan was a risk assessment program that is consistent with the National Institute of Standards and Technology's (NIST) Cybersecurity Framework,[96] designed to evaluate internal and external security threats and requiring a biennial report of its findings to the FCC.[97] Also included was a comprehensive information security program that documents who is given access to customers' propriety network information (CPNI), establishes safeguards to prevent unauthorized access or use of that data, and outlines sanctions for parties who disregard the guidelines set out in the program.[98] Additionally, the consent decree requires annual audits and periodic penetration testing of Cox's security systems, as well as the use of a site-to-site virtual private network (VPN) for use by third-party vendors who must access customer data in the course of business with Cox, among other procedures.[99] Cox also would be required to designate a compliance officer with senior management authority in its corporate structure, with the role of ensuring that Cox follows through with the compliance plan and consent decree.[100]

Following the enforcement approach of the *Cox* order, on October 27, 2016, the FCC adopted an order that granted the agency authority to regulate the data security practices of broadband and other telecommunications service providers.[101] The Privacy Order affirmed the need for clearer data privacy laws, and established a focus on transparency in data collection, consumer choice, and the maintenance of secure data systems as three crucial

93. *Id.* at 12309.

94. *Id.* at 12311.

95. *Id*. at 12310–16.

96. NAT'L INST. OF STANDARDS & TECH., *Framework for Improving Critical Infrastructure Cybersecurity*, NAT'L INST. OF STANDARDS & TECH. (Feb. 12, 2014), available at: http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf, [https://perma.cc/6VKA-64ZJ].

97. Cox, 30 FCC Rcd at 12310.

98. *Id.*

99. NAT'L INST. OF STANDARDS & TECH., *supra* note 96. Cox, 30 FCC Rcd at 12310 (pg. 8)

100. Cox, 30 FCC Rcd*Id.* at 12310.

101. In the Matter of Protecting the Privacy of Customers of Broadband and Other Telecommunications Services, *Report and Order*, FCC-16-148, para. 5 (2016), https://apps.fcc.gov/edocs_public/attachmatch/FCC-16-148A1_Rcd.pdf [https://perma.cc/W27E-WGLF], [hereinafter *Privacy Order*].

components of a viable legal framework.[102] The issues relating to transparency and choice, specifically regarding what types of data may be collected and what options consumers should have in permitting or refusing collection of their personal data, deal more with privacy than security. Policymaking over data privacy has generated its own debate that is separate from data security, despite the issues being intertwined.[103] Privacy concerns are thus related to the data collection process, while security concerns arise once a company is in possession of consumer data.

In addressing data security, the Privacy Order took a step back from the type of specific requirements imposed by the Enforcement Bureau in the 2015 order against Cox, and instead adopted a more general "reasonableness" approach similar to that of the FTC.[104] The lack of rigidity in the Privacy Order's security proposal stems from a concern that overly-detailed and inflexible guidelines could prove unsuited for keeping pace with technological advances, may unfairly burden smaller companies, or could reduce incentives for innovation and competition in developing security techniques.[105] It remains contentious whether or not a one-size-fits-all procedural standard could prove to be obstructive for companies with fewer resources to put toward new security measures.[106] The concern was that a comprehensive set of specific guidelines may be well-suited for larger carriers, but could present unnecessary costs for smaller providers.[107] Finally, the Privacy Order contemplated, but explicitly stopped short of implementing, safe harbors for companies that follow a predetermined set of "best practices" in data security and nonetheless suffer a breach. The rationale for refusing to implement safe harbors was that rigid adherence to an inflexible list of "best practices" would restrict the "reasonableness" standard from keeping pace with technological developments.[108] Though the Privacy Order was later overturned on April 3, 2017[109], it appears that legislators are reluctant to move away from the FTC's imprecise "reasonableness" standard for data security regulation.

102. *See id.* at para. 3; *see also* Margaret Harding McGill, *FCC, FTC Zero in on Data Security, Privacy*, LAW360 (Jan. 6, 2016, 8:27 PM EST), http://www.law360.com/articles/743314/fcc-ftc-chiefs-zero-in-on-data-security-privacy, at 2.

103. *See* Natasha Lomas, *FCC Urged to Rein in Broadband Providers on Privacy Grounds*, TECHCRUNCH, (Jan. 19, 2016), http://techcrunch.com/2016/01/19/fcc-urged-to-rein-in-broadband-providers-on-privacy-grounds/./, [https://perma.cc/CH8Z-W43S], at 1.

104. *See Privacy Order* at para. 236.

105. *See id.* at para. 235.

106. *See id.* at para. 241-42.

107. *See id.*

108. *See id.* at para. 249.

109. S.J. Res. 34, 115th Cong. (2017).

III. THE FTC SHOULD MOVE FORWARD WITH A SPECIFIC REQUIREMENTS ENFORCEMENT MODEL SIMILAR TO THE FCC'S APPROACH DEMONSTRATED IN *COX*

A legislative overhaul is sorely needed to fully address the modern importance of consumer data – not only as a preventative measure to abate the economic harms caused by breaches, but also to more effectively protect consumers who are directly affected by the exposure of their personal information. Currently, the FTC has rooted its data security enforcement authority (for industries not covered by the FCRA, COPPA, and GLBA) in Section 5 of the FTC Act, which makes no specific mention of consumer data.[110] The FTC has undertaken thorough efforts to provide businesses and consumers with up-to-date information on how to maintain effective data security practices.[111] However, given that the FTC's statutorily granted authority has left the agency with the vague "reasonableness" standard for investigating data breach cases, companies are left guessing at how a court will rule if their data practices are brought under judicial scrutiny. Indeed, the FTC itself has recognized the need for new legislation in this area. For example, the FTC has proposed to Congress "a data security bill to establish broadly applicable data security standards for companies and [to] require them, in certain circumstances, to notify consumers in the event of a breach."[112] It is true that rapid notification to consumers in the event of a breach is imperative so measures can be taken to mitigate any harm after personal information has been exposed.[113] But the goal should be to create a legal framework that places an emphasis on preventing breaches in the first place.

A. The FTC Needs to Provide Businesses with More Clarity on What Data Security Practices to Adopt, and When a Breach Should be Actionable

The *Wyndham Worldwide* case demonstrated that, while the FTC is certainly willing and able to enforce its authority to regulate the data security practices of companies, businesses are currently left to sift through the body of data breach enforcement actions in order to figure out what the FTC's "reasonableness" standard truly requires. The mere fact that the Third Circuit in *Wyndham* recognized the potential for unresolvable "borderline cases" illustrates the need for a concrete code of conduct.[114] If companies are uncertain as to what constitutes "reasonable" data security practices, then it is possible they could overlook certain crucial security measures as not being

110. 15 U.S.C. § 45 (2012)..

111. *Discussion Draft of H.R.__, Data Security and Breach Notification Act of 2015: Hearing Before the H. Comm. on Energy & Commerce, Subcomm. On Commerce, Mfg., & Trade*, 114th Cong. 7–9 (2014) (statement of Jessica Rich, DirectorDir. of the Bureau of Consumer ProtectionProt. at the FTC).

112. *Id*. at 9.

113. *Id*. at 10.

114. FTC v. Wyndham Worldwide Corp., 799 F.3d 236, 256 (3d3rd Cir. 2015).

conclusively "required", thereby opening themselves up to breaches that could have been prevented had there been universally applied standards. Why leave open the possibility for these borderline cases to be picked apart by courts in *response* to harmful breaches when a viable alternative is to lay out a specific set of technical and procedural requirements that represents the cutting edge in protective measures?

Up until the FCC's Privacy Order, the Enforcement Bureau's specific-requirements approach[115] had provided companies under the FCC's purview with perhaps the clearest and most specific model for an up-to-date data security program.The requirements that the Enforcement Bureau imposed on Cox "[did] not appear to be limited to remediating the particular alleged deficiencies that the FCC contended led to the data security breach."[116] Instead, the consent decree outlined what the Enforcement Bureau determined was the most effective set of security measures that a company can take to prevent *any* form of data breach – not just the type that Cox suffered.[117] This forward-looking approach at the time provided a sustainable data security solution not only for Cox, but for *any* business that wished "to avoid running afoul of the Enforcement Bureau."[118]

It is important to note that the Enforcement Bureau did not go so far as to dictate every detail of the new security regime for Cox to follow. Instead, it left room for flexibility, as long as Cox met the specific goals outlined in the decree and documented its security procedures.[119] This provided a relatively non-intrusive middle ground between the imprecise "reasonableness" standard currently promulgated by the FTC and one that is so painstakingly specific and restrictive that it would restrain Cox from conducting business effectively. Finally, the requirement that Cox integrate a compliance officer into the company's senior management structure, with the role of overseeing execution of the consent decree, is significant because it incorporates data security implementation into the core operations of the company.[120] Hiring a compliance officer at a high-level position also provides flexibility for the company, as it leaves the day-to-day execution of the consent decree, and further matters of data security, in the hands of Cox's leadership instead of imposing an onerous system of FCC oversight.[121] The mandatory designation of this officer, along with the narrower technical requirements addressed toward curing the cause of the breach, makes the

115. *See* Patrick H. Haggerty, F. Paul Pittman, *FCC's Growing Privacy and Data Security Enforcement, Data Privacy Monitor* (Dec. 8, 2015), http://www.dataprivacymonitor.com/enforcement/fccs-growing-privacy-and-data-security-enforcement/, [https://perma.cc/TYA3-NCL9].

116. ROPES & GRAY, *supra* note 11; *see also* Cox Commc'ns, Inc., 30 FCC Rcd 12302, 12310 (2015) (the designation of a compliance officer was a more general security requirement imposed by the FCC that was not specifically related to the phishing scheme that caused Cox to suffer the data breach).

117. *See generally* Cox, 30 FCC Rcd at 12302.

118. Haggerty, *supra* note 115.

119. *See* Cox, 30 FCC Rcd at 12311.

120. *See id.* at 12310.

121. *See id.*

order a more lasting and effective enforcement model than a general requirement of "reasonable" data security practices.

A statutory solution for the FTC, modeled after the Enforcement Bureau's approach in *Cox*, would be to enact a statute granting the FTC affirmative authority to regulate the data security practices of businesses in the U.S. generally, and granting the same to specialized agencies like the FCC. The new statute would (1) establish the FTC as the official U.S. DPA (while granting other agencies like the FCC affirmative data protection authority in their respective industries); (2) require the FTC to publish an annual list of guidelines that represent the most up-to-date security measures; (3) mandate the implementation of a safe harbor from breach actions for companies that follow the FTC's annual data security guidelines; (4) provide for a six-month grace period for companies to adapt to newly-published guidelines while remaining inside the safe harbor; and (5) form a system for adequately compensating consumers who fall victim to data breaches, either by requiring companies to pay victims directly, or by establishing a victims' fund that can be paid out of the U.S. Treasury in an instance where the company falls within the safe harbor.

This new legal framework would help to eliminate the issue of notice criticized in *Wyndham* by allowing the FTC to establish a legitimate foundation as the undisputed authority in the realm of data security, rather than forcing the FTC to overextend its rudimentary Section 5 "deceptive" and "unfair" acts powers to fill a regulatory void. The proposed statute would not necessarily mandate specific data security measures for companies to follow, but would instead give legal effect to the FTC's determination of what constitutes the current best practices in data security. The FTC would be required to periodically update a core list of data security practices that represent the most innovative and current means of protecting consumers' personal information – much in the way that the agency already does of its own volition.[122] For industries that are regulated by a specialized agency, like telecommunications for example, the relevant agency would be allowed to add to or clarify the FTC's list of requirements, but could not waive any of the FTC's specifications absent a showing that a certain requirement that places an undue burden for that industry.

The goal would be for the FTC to effectively assume the role of a standard-setting body in consumer data security, as businesses would presumably want to earn the statute's legal benefits by keeping their data systems up to date with the FTC's guidance. A potential advantage of having at least a semi-standardized set of data security measures across all U.S. businesses would be that systemic flaws could be identified rapidly. If one company suffers a breach or encounters problems due to an issue with the prevailing data security paradigm, then every other business that has adopted the same security measures would be able to pool their intellectual resources into fixing the issue and strengthening the overall system. To account for the evolution of technology and increasing sophistication of hackers, the FTC

122. *See Start with Security: A Guide for Businesses*, FTC (June, 2015) https://perma.cc/P7YY-GQYKwww.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf.

would be required to update its data security guidance on a yearly basis, much like how the Enforcement Bureau sought to require Cox to submit risk assessment reports on its security measures at least every two years.[123] Any concern that a standard set of security guidelines would reduce competition and innovation[124] is without merit; the rising cost of breaches and persistent threat of hackers will naturally continue to provide a market-based incentive for companies to stay ahead of the curve in protecting consumer data.[125] Additionally, to avoid the issue of constantly requiring companies that had met the FTC data security certification benchmark in previous years to overhaul their systems, the statute would provide for a grace period of six months to a year during which businesses could have extra time to adopt any new standards before losing its certification. This period could be shortened if there is so drastic a change in the FTC's guidelines, due to a flaw, innovation, or otherwise, that the previous year's security paradigm has already become obsolete. The statute would give the FTC discretion over when this would be the case.

The central goals of this proposal are to improve data security in U.S. commerce generally, to prevent data breaches, and to protect the individual consumer. The time is ripe for a genuine and focused legislative effort that aims to put the U.S. ahead of the curve on data security, particularly in a time when consumers are taking data privacy concerns into serious consideration when deciding the companies with which to do business.[126]

B. Data Breach Remedies Should Include Recourse for Consumers Commensurate with the Modern Value of Personal Data

Even with a more robust data security framework in place for businesses, a further component is required to ensure that consumers can seek adequate remedies in the event of breach. The Seventh Circuit in *Remijas* recognized that assessing the harm caused to individual consumers who are affected by a data breach is difficult, especially when the personal information has not yet been used to their detriment.[127] While the plaintiffs in *Remijas* were able to recover against Neiman Marcus, both for damages incurred in trying to mitigate the harm caused by the breach as well as the for the risk of future harm,[128] the Court held that there could be no recovery for an injury in the abstract, "particularly since the complaint did not suggest that the plaintiffs could sell their personal information for value."[129] This seems to conflict with the Court's own statement when, in response to Neiman Marcus' assertion that a data breach did not constitute a substantial risk of future harm

123. *See* Cox Commc'ns, Inc., 30 FCC Rcd 12302, 12310 (2015).
124. *See Data Privacy NPRM* at para. 179.
125. *See 2015 Cost of Data Breach Study: Global Analysis*, Ponemon Institute, May 2015, at 2.
126. *See* Conradt, *supra* note 3, at 1.
127. Remijas v. Neiman Marcus Grp., LLC, 794 F.3d 688, 693–94 (7th Cir. 2015).
128. *Id.* at 693-95.
129. *Id.* at 695.

for those affected, it posed the rhetorical question: "[w]hy else would hackers break into a store's database and steal consumers' private information?"[130]

What the court failed to recognize in concluding that a data breach could not cause a harm to consumers other than through mitigation damages or future potential harm, is that personal data *does* carry an inherent value that the individual can monetize.[131] Consumers are already able to independently sell their personal information to companies that act as a middle-man for selling to data-collecting and processing entities and it is likely that these opportunities for consumers to "operate their own digital enterprises" will only become more numerous as awareness increases.[132] Thus, the loss of personal data can correspondingly constitute an economic loss if the original owner is no longer in control of it.[133] However, thus far, only a small number of people realize what monetary value their personal data holds.[134] Though Neiman Marcus, in its petition for *en banc* review, raised the issue of a potential split between the Seventh and Third Circuits,[135] the latter's holding in *Wyndham* indicates that the court agrees a data breach should be actionable even where no harmful use of the data has manifested.[136] Further, there is evidence that hackers will often wait before using any stolen data to commit fraud in order to avoid detection.[137] This suggests that even absent immediate harm caused to consumers affected by a breach, there is still a very substantial threat that some harm will manifest at some unknown point in the future.

Should the FTC develop a sustainable regulatory framework to handle the data security practices of companies across the U.S., it must, in an effort to protect the interests of consumers who suffer the effects of a data breach, integrate remedies into the framework that fully reflect the loss of economic value caused by a breach. Given that consumers are becoming more aware of personal data's inherent value and the increasing means by which personal data can be put to use for the individual,[138] a set of private remedies that the FTC could choose to update over time would conceivably work well to empower consumers with more control over their information in the marketplace. While these remedies could remain flexible under the discretion

---

130. *Id.* at 693.

131. *See* Tim Cooper & Ryan LaSalle, Guarding and Growing Personal Data Value, Accenture (2016) at 14.

132. *See id.* at 14 ("As individuals become more aware of the potential to monetize their data—and as channels for doing so become more accessible—they will be able to operate as their own digital enterprises, treating their data as a business would manage its intellectual property. For example, intermediaries … enable users to sell their data by connecting their social media and debit and credit card accounts to businesses that want to gather quality data about their target customers").

133. *See id.* at 14.

134. *See id.* at 14.

135. Joey Godoy, *7th Circ. Won't Revisit Neiman Marcus Data Breach Ruling*, LAW360 (Sept.Sep 17, 2015, 5:29 PM EDT), http://www.law360.com/articles/704243/7th-circ-won-t-revisit-neiman-marcus-data-breach-ruling.

136. FTC v. Wyndham Worldwide Corp., 799 F.3d 236, 246 (3d Cir. 2015).

137. Matthew Goldstein & Nicole Perlroth, *Authorities Closing in on Hackers Who Stole from JPMorgan Chase*, N.Y. TIMES (Mar. 15, 2015), http://www.nytimes.com/2015/03/16/business/dealbook/authorities-closing-in-on-hackers-who-stole-data-from-jpmorgan-chase.html?_r=0, [https://perma.cc/BP5B-QE86].

138. *See* Cooper & LaSalle, *supra* note 131, at 14.

of the FTC, there are several possible options that could also work from the outset.

The best method of compensating consumers whose personal data has been breached would be to pay out monetary damages for the immediate harm, and to provide services that mitigate potential future harm from illicit use of the data. An effective solution to calculate the monetary damages would be to fine companies at a rate corresponding to the volume and value of data lost, paid into a fund to be distributed among the affected consumers. For example, if a retailer suffers a breach, the compensation would be greater for financial and personally identifiable information, like credit card numbers, names, and addresses, than it would be for data that cannot directly be used to commit identity theft, like shopping history. Exact valuation may be difficult to calculate, though the existing market for consumer data bought and sold among companies could serve as a viable reference point.[139] A more punitive method would be to fine the liable company in the same way as previously discussed, except by calculating the damages as a percentage of profit that was realized by the company. The rationale behind this would be that the company charged its customers a premium for its goods and services yet chose not utilize those funds towards providing adequate data security measures (a rationale for damages raised and ultimately rejected by the court in *Remijas*).[140] Applying this method to the above example, the retailer would pay a percentage of the total profits made from its transactions with the specific customers who fell victim to the breach. The method that fines companies according to the value of data lost is the preferable choice, as it directly corresponds with the actual damages. The profit-based method, on the other hand, may produce unfair results if one company dealing in luxury goods has to pay a much greater fine than a company dealing in less expensive goods, even though the two suffer a breach of the same severity from the customers' standpoint.

In addition to applying monetary damages to account for the calculable losses from a breach, further redress should include equitable relief to compensate for the increased vulnerability of data theft victims. To address the threat of future harm faced by a consumer who has lost personal data, the company should pay for an identity protection or credit monitoring service. Neiman Marcus recognized the need to mitigate such future harm as it provided credit monitoring services to its customers after the breach, and before the class action suit went to trial.[141] This form of amends would ideally maintain or restore consumer confidence in the security of the market moving forward, in addition to purely rectifying the immediate economic harms caused by a given breach.

---

139. *See id.* at 8 (42% of the businesses currently gather personal data through commercial or data-sharing agreement with other organizations; 33% of the businesses currently purchase personal data from third-party data suppliers).

140. Remijas v. Neiman Marcus Grp., LLC, 794 F.3d 688, 695-96 (7th Cir. 2015) ("[W]e refrain from deciding whether the overpayment for Neiman Marcus products and the right to one's personal information might suffice as injuries under Article III.").

141. *Id.* Remijas, 794 F.3d at 694.

One potential issue with the proposed framework is determining what do to in the event that a company is in compliance with the FTC's up-to-date standards and nonetheless suffers a data breach. Assuming that there was no negligent action on the part of the company, and the presumption against liability holds up, the FTC could be faced with the issue of how to provide a remedy for the affected consumers who have suffered a harm from the breach. The statute would resolve this by establishing a "victim's fund" for such a scenario, which would be funded out of the U.S. Treasury using a percentage of all fines levied against businesses for previous data breaches, or from general taxpayer funds if that pool of fines is inadequate. The victim's fund would ensure that there is at least some recourse for the affected consumers. However, the new regulation's primarily goal would be to maintain such a strong set of data security standards that no company that followed the FTC's guidelines would suffer a breach.

One final aspect of the FTC's current data security authority that would need to be overhauled is the classification of different types of personal data. Currently, several statutes grant the FTC specific authority to regulate the data security practices of companies within certain industries or to enforce regulations against certain types of protected data.[142] It may be time to reexamine these specialized statutes, as it is now evident that all types of personal data potentially carry tangible economic value for the owner.[143] In FCC Commissioner Ajit Pai's dissent to the *Data Privacy NPRM*, Pai criticized the proposed data privacy and security rules as unjustifiably imposing stricter guidelines on Internet Service Providers (ISPs) than members of other industries that collect the same types of consumer data.[144] A baseline regulatory scheme should be designed to encourage full protection of all data that has been collected from consumers, and ISPs along with any other business must be held to a higher standard than what currently exists. While it would certainly be unfair to only impose new rules on ISPs, an FTC-led effort to establish a universal data security standard across all industries would meet the dual purpose of ensuring the effective protection of consumer data while also maintaining a level commercial playing field.

An apparent impediment to the establishment of stronger data security measures is the closely-related yet highly contentious issue of data privacy. Matters of data privacy concern the scope of a company's ability to use consumer data, as opposed to the extent of its obligations to protect consumer data from unauthorized third parties. Issues like transparency and consumer choice in data collection are matters that relate strictly to privacy, and they deserve to be addressed. However, ensuring the protection of all consumer information is a necessary starting point. In our increasingly digital world, consumers will continue to distribute their payment information on a massive scale, and the protection of such commonly shared data should not be hindered while legislators battle over the more complex privacy issues regarding such data. If companies cannot be trusted to keep their customers'

142. *See, e.g.*, Fair Credit Reporting Act, 15 U.S.C. § 1641 (1970); Children's Online Privacy Protection Act, 15 U.S.C. §§ 6501–6506 (1998); Financial Services Modernization Act, Pub.L. 106–102 (1999).

143. *See* Cooper & LaSalle, *supra* note 131, at 14.

144. *Data Privacy NPRM* at 139 (Comm'r Pai, dissenting).

data safe from unauthorized access, then there can be no meaningful discussion on what types of data may be collected or how. Consumers would assume that any data they share with a business can easily fall into the wrong hands, and the resulting mistrust could prevent personal data from becoming the immense market that it has the potential to be.

IV. CONCLUSION

It is time for Congress to move forward with new legislation that grants the FTC statutory authority over the data security practices of U.S. businesses. The current "reasonableness" standard under which the FTC holds companies accountable for data breaches is outdated, does not provide sufficient guidance on what data security measures to take, and does not adequately protect the consumers who are directly harmed by data breaches.

The FCC Enforcement Bureau has provided a promising model for data security enforcement that applies specific, forward-looking, technical, and procedural requirements that not only seek to prevent future data breaches, but also allow companies a measure of flexibility in how they implement the recommended practices. Congress should enact new legislation that will assist the FTC in moving away from its vague "reasonableness" standard toward creating a specific set of security guidelines that remain up-to-date and provide companies with affirmative incentives for following them.

If the FTC can encourage businesses to employ cutting-edge data security practices, then breaches can be mitigated, as data systems grow more complex and personal information becomes an increasingly valuable economic asset. Maintaining a domestic market that is safe from hacks and data breaches will result in greater consumer trust in the economy, and will empower the individual to enjoy full control of a valuable asset that has thus far only served to benefit third parties.