BLAMING THE VICTIM: HOW FTC DATA SECURITY ENFORCEMENT ACTIONS MAKE COMPANIES AND CONSUMERS MORE VULNERABLE TO HACKERS

David C. Grossman[*]

INTRODUCTION

In 2013, Target was the victim of a massive data breach that exposed the credit and debit card data of over 70 million customers.[1] This breach forced Target to pay a $10 million settlement to consumers and a $67 million settlement to credit card vendors, and it also created untold negative publicity for the retailer.[2] Target's breach is just one example in a steady parade of headlines revealing devastating data breaches at large retailers, putting the financial, personal, and health data of millions of consumers at risk.[3] In response, the federal government, primarily through the consumer protection authority of the Federal Trade Commission ("FTC" or "the Commission"),[4] as well as many state governments,[5] has pursued enforcement actions designed to hold companies accountable for negligent data storage practices and increase the overall level of data security in the private sector. But is imposing massive liability on a company that falls victim to a data breach truly the best way to protect consumer data?

---

[*] George Mason University School of Law, J.D. Candidate, May 2017; Articles Editor, GEORGE MASON LAW REVIEW 2016-2017; University of Chicago, A.B. Political Science, 2009. Special thanks to Anna Gentry, Camilla Hundley, and Patrick Pennella for their help in publishing this article.

1 Charles Riley & Jose Pagliery, *Target Will Pay Hack Victims $10 Million*, CNN MONEY (Mar. 19, 2015), http://money.cnn.com/2015/03/19/technology/security/target-data-hack-settlement/; Jose Pagliery, *Target Hack is a Wake Up Call on Privacy*, CNN MONEY (Jan. 11, 2013), http://money.cnn.com/2014/01/11/technology/security/target-hack-privacy/.

2 Chris Isidore, *Target and Visa Reach $67 Million Deal in Hacking Case*, CNN MONEY (Aug. 18, 2015), http://money.cnn.com/2015/08/18/news/companies/target-visa-hack-deal/; Riley & Pagliery, supra note 1

3 *See, e.g.*, Nick Turner, *Wendy's Says Breach Was 'Considerably' Bigger Than It Thought*, BLOOMBERG TECH. (June 9, 2016), http://www.bloomberg.com/news/articles/2016-06-09/wendy-s-says-breach-was-considerably-bigger-than-it-thought; Mary-Ann Russon, *Acer Online Store Hacked: Customers' Credit Card Details and Private Data Exposed*, INT'L BUS. TIMES (June 17, 2016), http://www.ibtimes.co.uk/acer-online-store-hacked-customers-credit-card-details-private-data-exposed-1566077; Aruna Viswanatha, *Morgan Stanley Fined $1 Million For Client Data Breach*, WALL ST. J. (June 8, 2016), http://www.wsj.com/articles/morgan-stanley-fined-1-million-for-client-data-breach-1465415374.

4 *E.g.*, FTC, PRIVACY & DATA SEC. UPDATE: 2015 1–2, 4, 15 (Jan. 2016), https://www.ftc.gov/reports/privacy-data-security-update-2015#data. *See also infra* Sections I.B.1-2.

5 *See infra* Section I.B.3.

Given the recent data breach suffered by the Office of Personnel Management, it is clear that not even the federal government is safe from a catastrophic data breach revealing the personal information of millions of Americans.[6] Indeed, many industry experts acknowledge that today it is a matter of when, not if, a company's data will be breached.[7] In this environment, where independent hackers, organized crime groups, and foreign governments are constantly developing more sophisticated hacking tools, how can the government distinguish between those companies that were truly negligent and those that were simply unlucky? Conversely, how can a company know how much security is necessary to avoid a government enforcement action or massive civil liability when even the most careful institutions may still be victimized by hackers?

The FTC has attempted to answer these questions by pursuing action against companies that fail to engage in reasonable data security practices, but for many companies and industries, what constitutes a reasonable data security plan remains uncertain.[8] The Third Circuit's recent decision in *FTC v. Wyndham Worldwide Hotel Corp.*[9] affirmed that the FTC has no obligation to provide specific guidance on what constitutes an unreasonable security program.[10] But many businesses and commentators still do not feel that the FTC's past actions and guidance are truly enough to guide cybersecurity practices and encourage better protection of consumer data.[11] Given the uncertainty created by the current data security regime, both the White House and Congress have acknowledged the need to create a uniform standard of care and a predictable enforcement regime to improve security and create certainty for companies.[12]

This comment analyzes the current federal regulatory scheme that governs data security. Part I describes the current state of data security including administrative, statutory, and industry-led regulatory regimes that seek to improve the standards of protection of consumer data. This includes

---

6 *See, e.g.*, Lisa Weintraub Schifferle, *OPM Data Breach – What Should You Do?*, FTC: CONSUMER INFORMATION (June 4, 2015), https://www.consumer.ftc.gov/blog/opm-data-breach-what-should-you-do.

7 *See, e.g.*, Jose Pagliery, *Welcome to the Age of Hacks*, CNN MONEY (Sept. 4, 2014), http://money.cnn.com/2014/09/04/technology/security/age-of-the-hack/.

8 *See, e.g.*, FTC v. Wyndham *Worldwide Corp.*, 799 F.3d 236, 259 (3d Cir. 2015). *See also* Allison Grande, *Landmark FTC Win Fuels Uncertainty For Data Breach Targets*, LAW360 (Apr. 8, 2014), http://www.law360.com/articles/526164/landmark-ftc-win-fuels-uncertainty-for-data-breach-targets; Alden Abbott, *Wyndham Decision Highlights FTC Role in Cybersecurity: Legal and Policy Considerations*, TRUTH ON THE MARKET (Sept. 1, 2015), http://truthonthemarket.com/2015/09/01/wyndham-decision-highlights-ftc-role-in-cybersecurity-legal-and-policy-considerations/.

9 799 F.3d 236 (3d Cir. 2015).

10 *Id.* at 259.

11 *E.g.*, Grande, *supra* note 8; Abbott, *supra* note 8.

12 *See* John D. McKinnon, *Lawmakers, White House Near Cybersecurity Agreement*, WALL ST. J. (Dec. 15, 2015), http://www.wsj.com/articles/lawmakers-white-house-near-cybersecurity-agreement-1450219168.

an examination of the FTC's statutory authority and the case law built up around it,[13] as well as federal and state statutes that govern the standard of care for data security.[14] Part II analyzes the current state of FTC regulation and attempts to identify what the prevailing standard of care is for data security in the private sector. Part III offers a normative analysis of the current state of data security regulation and argues that the current regime is incoherent and provides little specific guidance, which creates uncertainty that ultimately undermines the overall level of data security in the private sector. Part III also offers recommendations on the provision of a potential federal statutory solution to provide clarity to corporations who store data and encourage information sharing through limited liability that will ultimately raise the level of security for consumer data.

I. BACKGROUND – CURRENT THREATS AND REGULATION IN DATA SECURITY

As companies began to collect and store more customer data, identity theft and privacy harms became a problem of increasing concern for consumers, companies, and regulators.[15] Initially, Congress, federal agencies, and state governments focused their efforts on specific industries where data was deemed especially sensitive, such as healthcare and finance.[16] However, because companies in every industry now collect an increasing amount of personal data to improve their services and marketing, private industry and the government have struggled to respond to the increasing likelihood that consumers will have their data exposed to threats as a consequence of everyday transactions and activities.[17] This section examines the current state of data security—including the threats facing companies that collect personal data—as well as the solutions put in place by Congress, federal agencies, and state regulators to combat these threats.

---

13 *See, e.g.*, 15 U.S.C. § 45 (2012); *Wyndham Worldwide Corp.,* 799 F.3d 236; *Orkin Exterminating Co. v. FTC*, 849 F.2d 1354 (11th Cir. 1988); *Am. Fin. Servs. Assoc. v. FTC*, 767 F.2d 957 (D.C. Cir. 1985).

14 *See* Fair and Accurate Credit Transaction Act of 2003, Pub. L. No. 108–159, 117 Stat. 1952 (codified as amended at 15 U.S.C. § 1681c-1 (2012)); Gramm-Leach-Bliley Act, Pub. L. No. 106–102, 113 Stat. 1338 (1999) (codified as amended in scattered sections in 15 U.S.C. (2012)); Children's Online Privacy Protection Act of 1998, Pub. L. No. 105–277, 112 Stat. 2681–728 (1998) (codified as amended in scattered sections in 15 U.S.C. §§ 6501 *et sec.* (2012)).

15 The Identity Theft Resource Center, which tracks and categorizes data breaches, reports that from 2005 to Apr 18, 2016 there have been 6,079 data breaches compromising 862,527,023 records, with the number of breaches increasing each year. IDENTITY THEFT RES. CTR, DATA BREACHES, http://www.idtheftcenter.org/id-theft/data-breaches.html (last visited June 18, 2016).

16 *See, e.g.*, Fair and Accurate Credit Transaction Act; Gramm-Leach-Bliley Act.

17 *See Data, Data Everywhere*, ECONOMIST (Feb. 27, 2010), http://www.economist.com/node/15557443.

A. *The Crisis in Data Security*

Data breaches of major companies have become a growing problem as an increasing number of consumers give sensitive personal, financial, and health information to a wide variety of companies every day. As a result, every year brings more massive breaches drawing headlines, with millions of consumer records exposed.[18] In 2015, there were at least 781 data breaches reported in the United States,[19] exposing over 169 million individual consumer records.[20] These breaches targeted financial institutions, major retail corporations, universities, health care providers, and government agencies, both local and federal.[21] This follows a record high of 783 data breaches reported in 2014, itself a 27.5 percent increase over the previous year, with almost 850 million records exposed since 2005.[22] These numbers are deeply concerning, but they actually underestimate the problem. This is because many institutions are not required by law to report data breaches and may choose not to report to avoid "the financial dislocation, liability and loss of goodwill that comes with disclosure and notification."[23]

The possibility of a data breach and its attendant risks to consumers of identity theft, fraud, and privacy violations are only increasing as individuals store more sensitive data electronically with organizations that may lack adequate security practices.[24] Many organizations entrusted with personal consumer data do not practice basic tenets of data security, such as storing only the minimum amount of data needed to fulfill the purpose of their

---

18 *See generally* IDENTITY THEFT RES. CTR, DATA BREACHES, http://www.idtheftcenter.org/Data-breaches/data-breaches.html (last visited June 18, 2016) (offering annual reports showing yearly increases in number of data breaches and records compromised). *See, e.g.*, IDENTITY THEFT RES. CTR, DATA BREACH REPORTS 15 (June 14, 2016) [hereinafter 2016 DATA BREACH REPORT] (473 breaches exposing 12.6 million records), http://www.idtheftcenter.org/Data-breaches/data-breaches.html; IDENTITY THEFT RES. CTR, DATA BREACH REPORTS 24 (Dec. 31, 2015) [hereinafter 2015 DATA BREACH REPORT] (781 breaches exposing 169 million records), http://www.idtheftcenter.org/Data-breaches/2015data-breaches.html.

19 The Identity Theft Research Center defines a data breach as "an incident in which an individual name plus a Social Security number, driver's license number, medical record or financial record (credit/debit cards included) is potentially put at risk because of exposure." 2016 DATA BREACH REPORT, *supra* note 18, at 2.

20 2015 DATA BREACH REPORT, *supra* note 18, at 24.

21 *Id.* at 3–4.

22 Press Release, Identity Theft Res. Ctr., Identity Theft Resource Center Breach Report Hits Record High in 2014, (Jan. 12, 2015) (675 million records compromised since 2005), www.idtheftcenter.org/ITRC-Surveys-Studies/2014databreaches.html; 2015 DATA BREACH REPORT, *supra* note 18, at 4 (an additional 170 million records compromised in 2015).

23 Press Release, Identity Theft Res. Ctr., *supra* note 22. *See also* GINA STEVENS, CONG. RESEARCH SERV., R42475, DATA SEC. BREACH NOTIFICATION LAW (2012) (listing the prominent laws relating to data security breaches).

24 Lucy L. Thomson, *Cybercrime and Escalating Risks*, *in* DATA BREACH & ENCRYPTION HANDBOOK 3, 7–8 (Lucy Thomson ed., 2011).

business.[25] The data put at risk is frequently personally identifiable, and includes bank account and social security numbers, medical records, financial records, legal records, and information on mortgages and consumer loans.[26] Breaches of this sensitive, personally-identifiable data have only become more likely with the increasing number of transactions involving personal information that now take place on mobile devices and cloud services.[27] High profile data breaches became so commonplace in 2014 that one IBM report labeled it "The year the Internet fell apart."[28]

This section lays out the current data security crisis, examining the overall impact of recent data breaches and highlighting the specific effects of a number of recent high profile breaches affecting companies such as Sony, Target, Experian, and T-Mobile. These case studies will serve to illustrate the potentially devastating impact of a breach on consumers, corporations, and the economy as a whole. Additionally, this section examines some of the prevailing data security standards that have been adopted by the government and industry to combat these catastrophic breaches.

1. Anatomy and Consequences Recent High Profile Consumer Data Breaches

The threat of a data breach can come from a variety of sources, and depending on the context, can bring regulatory scrutiny, civil liability, and severe harm to a company's business and reputation. A recent report by the Ponemon Institute and IBM estimated that the per capita cost of a data breach in the U.S. is $221 per compromised consumer data record, which includes remediation costs, reputation loss, and investigative and legal services.[29] The potential dangers and consequences inherent in current business data collection practices are apparent in some of the recent high-profile data breaches that have attracted the attention of regulators, tort lawyers, and the news media. These recent breaches illustrate the potential threats that companies face, as well as the financial and reputational losses they incur as a result of a large-scale breach of consumer data.

---

25 *Id.* at 8.

26 *Id.* at 8–13.

27 *Id.* at 12–13.

28 IBM, IBM 2015 CYBERSECURITY INTELLIGENCE INDEX 3 (July 2015), http://www-03.ibm.com/security/data-breach/2015-cyber-security-index.html.

29 PONEMON INST., 2016 COST OF DATA BREACH STUDY: GLOBAL ANALYSIS 1–2, 26–27 (June 2016) (finding that the average cost of a data breach is $4 million and $158 per record, based on 383 companies in 12 countries), http://www-03.ibm.com/security/data-breach/index.html.

a. *Sony Online Entertainment (April 2011)*

On April 19, 2011, Sony shut down a number of its online entertainment services, including the popular PlayStation Network ("PSN") service, without notice after discovering an intrusion into its network that had occurred days earlier.[30] Sony determined that the intrusion affected over 77 million users, leading to the exposure of customer names, addresses, email addresses, passwords, birth dates, and credit card and bank account information by hackers.[31] Although Sony stored its customers' credit card information in an encrypted database, it did not encrypt customers' personal information, exposing a huge amount of personal data to hackers.[32] Subsequently, the breach forced Sony to spend close to $171 million on network upgrades, customer support, and legal costs associated with the breach, and it was the subject of over 50 class action lawsuits in addition to fines imposed by international regulators.[33] Overall, one industry expert estimated that the hack may have cost Sony more than $250 million through the end of 2012.[34]

b. *Target (2013)*

On December 19, 2013, Target announced that it had been the victim of a data breach in its Point of Sale ("POS") system used to process credit cards at the height of the holiday shopping season.[35] The breach led to the theft of an estimated 40 million credit card records and another 70 million personal records, including names, addresses, email addresses, and phone numbers, over the course of several weeks.[36] Investigators traced the attack to an email malware program targeting, not Target itself, but a heating, air conditioning, and refrigeration firm that Target had given network access

---

30 Martyn Williams, *PlayStation Network Hack Timeline*, PCWORLD (May 1, 2011), http://www.pcworld.com/article/226802/playstation_network_hack_timeline.html. *See also* Liana B. Baker & Jim Finkle, *Sony PlayStation Suffers Massive Data Breach*, REUTERS (Apr. 26, 2011) (noting also that Sony did not disclose the breach to the public for seven days), http://www.reuters.com/article/us-sony-stoldendata-idUSTRE73P6WB20110427.

31 Baker & Finkle, *supra* note 30.

32 Williams, *supra* note 30.

33 John Gaudiosi, *Why Sony Didn't Learn From its 2011 Hack*, FORTUNE (Dec. 24, 2014), http://fortune.com/2014/12/24/why-sony-didnt-learn-from-its-2011-hack/; Danielle Walker, *Sony to Shell Out $15M in PSN Breach Settlement*, SC MAGAZINE (Jul. 24, 2014), http://www.scmagazine.com/sony-to-shell-out-15m-in-psn-breach-settlement/article/362720/.

34 Gaudiosi, *supra* note 33.

35 Robin Sidel et al., *Target Hit By Credit-Card Breach,* WALL ST. J. (Dec. 19, 2013), http://www.wsj.com/articles/SB10001424052702304773104579266743230242538.

36 Brian Krebs, *The Target Breach, By the Numbers*, KREBS ON SEC. (May 6, 2014), http://krebsonsecurity.com/2014/05/the-target-breach-by-the-numbers/ [hereinafter Krebs, *Target Data Breach*].

to, despite the fact that the company relied on a free anti-malware program for security.[37] The consequences for Target were dramatic, with the breach leading to a 46% drop in quarterly profits, $100 million spent to upgrade payment terminals, and the resignation of Target's Chief Executive Officer, Chief Information Security Officer, and Chief Security Officer.[38] Additionally, the breach left Target open to a civil suit by credit card issuers, with Target settling with Visa for $67 million and over $39 million with MasterCard and other credit card issuers to compensate for the over $200 million spent by the credit card vendors to re-issue stolen credit cards.[39]

c. *Experian and T-Mobile (2015)*

In October 2015, credit bureau and data broker Experian disclosed another major breach of consumer data from customers who applied for financing through wireless provider T-Mobile.[40] The breach exposed an estimated 15 million customer records, including social security numbers, names, and dates of birth, although Experian stated that no payment or banking information was stolen.[41] While the source of the breach remains undiscovered, industry experts estimate that it lasted for two years, beginning in 2013, and industry press has accused the credit bureau of aggressively acquiring other data brokerage firms at the expense of consumer data security.[42] As a result, Experian has offered customers free credit monitoring service, and the Senate Banking Committee appears likely to investigate the company's practices.[43] While this breach is in its early stages of investi-

---

37 Brian Krebs, *Email Attack on Vendor Set Up Breach at Target*, KREBS ON SEC. (Feb. 12, 2014), http://krebsonsecurity.com/2014/02/email-attack-on-vendor-set-up-breach-at-target/.

38 Krebs, *Target Data Breach*, *supra* note 36.

39 Kevin M. McGinty, *Target and Card Issuers Reach Final Data Breach Settlement*, NAT'L L. REV. (Dec. 12, 2015), http://www.natlawreview.com/article/target-and-card-issuers-reach-final-data-breach-settlement; Robin Sidel, *Target to Settle Claims Over Data Breach*, WALL ST. J. (Aug. 18, 2015), http://www.wsj.com/articles/target-reaches-settlement-with-visa-over-2013-data-breach-1439912013; Christine DiGangi, *The Target Breach Has Cost Banks $240 Million . . . So Far*, CREDIT.COM (Feb. 21, 2014), http://blog.credit.com/2014/02/target-data-breach-cost-banks-240-million-76636/.

40 Experian, *Experian Notifies Consumers in the U.S. Who May Have Been Affected By Unauthorized Acquisition of a Client's Data*, PR NEWSWIRE (Oct. 1, 2015), http://www.prnewswire.com/news-releases/experian-notifies-consumers-in-the-us-who-may-have-been-affected-by-unauthorized-acquisition-of-a-clients-data-300152926.html.

41 *Id*.

42 Brian Krebs, *Experian Breach Affects 15 Million Consumers*, KREBS ON SEC. (Oct. 2, 2015), http://krebsonsecurity.com/2015/10/experian-breach-affects-15-million-consumers/; Brian Krebs, *At Experian, Security Attrition Amid Acquistions*, KREBS ON SEC. (Oct. 2, 2015), http://krebsonsecurity.com/2015/10/at-experian-security-attrition-amid-acquisitions/.

43 Ken Sweet, *Senator Presses Experian to Disclose Details of Data Breach That Affected T-Mobile Customers*, U.S. NEWS & WORLD REP. (Oct. 14, 2015), http://www.usnews.com/news/business/articles/2015/10/14/senator-calls-for-experian-to-share-details-on-data-breach.

gation, because of the sensitivity of the data involved, federal and state regulators will likely take a close look at the practices that led to an apparent two-year exposure of sensitive customer data.

These examples show the breadth of a growing data security crisis that impacts both companies and consumers. While the threat of data breaches continues to grow, there are steps that companies can take to protect consumer data, and a number of different standards exist for best practices that agencies and courts can rely upon when attempting to determine which companies are negligent with consumer data and which were simply the unlucky victims of a sophisticated hack.

2. Current Industry Data Security Practices

A variety of standards and best practices exist to inform a company's data security program, though none offer complete protection.[44] Most standards include three main elements: (1) some classification of personal data and an assignment of value or sensitivity to it, (2) best practices for managing and minimizing vulnerabilities to that data, and (3) procedures for response to potential vulnerabilities and breaches to minimize damage to consumers.[45] This section examines some of the leading industry standard regimes used to ensure data security, and illustrates the variety of approaches to data security currently prominent in private industry and government.

a. *Payment Card Industry Data Security Standards*

In light of the potential severity of a breach in consumer financial data, the credit card industry was an early adopter of data security standards, creating the Payment Card Industry Security Standards Council and issuing its first Data Security Standards ("PCI DSS") in 1996.[46] Since that time, many industries and regulators have looked to PCI DSS as a barometer for industry best practices, with Nevada becoming the first state to mandate PCI DSS compliance for businesses accepting credit cards in 2010.[47] Commentators have suggested that PCI DSS could serve as a basis for the stan-

---

44 *See, e.g.*, Nate Lord, *Most Important Next Steps You Should Take After a Data Breach in 2014-2015 & Beyond,* DIGITAL GUARDIAN (May 18, 2016) (summarizing data security advice from 30 data security experts), https://digitalguardian.com/blog/data-breach-experts-share-most-important-next-step-you-should-take-after-data-breach-2014-2015.

45 Lucy L. Thomson, *Despite the Alarming Trends, Data Breaches Are Preventable*, *in* DATA BREACH & ENCRYPTION HANDBOOK 17, 28–30 (Lucy Thomson ed., 2011).

46 Arthur E. Peabody, Jr. & Renee A. Abbott, *The Aftermath of Data Breaches: Potential Liability and Damages*, *in* DATA BREACH & ENCRYPTION HANDBOOK 31, 28–30 (Lucy Thomson ed., 2011).

47 *Id.*

dard of reasonable security used by courts to determine whether a company has been negligent in its data security practices.[48]

PCI applies two sets of standards: one to software applications (Payment Application Data Security Standard ("PA-DSS")) and one to merchants accepting credit cards ("PCI DSS").[49] Each one has varying requirements, and compliance with PA-DSS does not mean compliance with PCI-DSS.[50] Generally, PCI DSS requires businesses that wish to accept payment cards from its member issuers (American Express, Discover, JCB, International, MasterCard, and Visa) to maintain a secure network, a vulnerability management system, access control measures, a regularly updated information security policy, and networks regularly tested for vulnerabilities.[51] While this overall framework applies to all merchants wishing to accept credit cards, it requires each individual member brand to maintain its own compliance program for its merchant customers, and each brand is expected to monitor its respective merchant customers for compliance.[52]

While PCI DSS could serve as a model for application of standards, it remains limited by being industry-specific.[53] It is also largely a self-regulated system managed by the major credit card issuers, so it lacks the broad applicability sought by federal and state regulators.[54] As such, the federal government has made efforts to create a broader set of standards with the National Institute of Standards and Technology's 2014 Cybersecurity Framework.[55]

---

48 *See, e.g.*, Scott J. Shackelford et al., *Toward a Global Cybersecurity Standard of Care? Exploring the Implications of the 2014 NIST Cybersecurity Framework on Shaping Reasonable National and International Cybersecurity Practices*, 50 TEX. INT'L L.J. 305, 339–40 (2015); Michael L. Rustad & Thomas H. Koenig, *The Tort of Negligent Enablement of Cybercrime*, 20 BERKELEY TECH. L.J. 1553, 1588–89 (2005).

49 *See* Peabody & Abbott, *supra* note 46, at 46; PCI SSC Data Security Standards Overview, PCI SEC. STANDARDS COUNCIL, https://www.pcisecuritystandards.org/pci_security/standards_overview (last visited June 26, 2016).

50 *Compare* PCI SEC. STANDARDS COUNCIL, PAYMENT CARD INDUSTRY (PCI) DATA SECURITY STANDARDS: REQUIREMENTS AND SECURITY ASSESSMENTS PROCEDURES 3-4, 5, 9 (2016) [hereinafter PCI-DSS PROCEDURES] (PCI-DSS requirements) *with* PCI SEC. STANDARDS COUNCIL, PAYMENT CARD INDUSTRY (PCI) PAYMENT APPLICATION DATA SECURITY STANDARDS: REQUIREMENTS AND SECURITY ASSESSMENTS PROCEDURES 3, 5 (2016) [hereinafter PA-DSS Procedures] (PA-DSS requirements).

51 PCI-DSS PROCEDURES, supra note 50, at 3–5.

52 Peabody & Abbott, *supra* note 46, at 46.

53 *See* Rustad & Koenig, *supra* note 48, at 1588 (noting how the financial services industry developed PCI standards electronic payments).

54 *Id.* (noting how the PCI standard is a private standard used by the financial services industry).

55 *See* discussion *infra* Section I.A.2.b

b. *National Institute of Standards and Technology – Cybersecurity Framework*

In February 2014, The National Institute of Standards and Technology ("NIST") released its *Framework for Improving Critical Infrastructure Cybersecurity* ("Framework"), [56] which "harmonizes consensus standard and industry best practices to provide, its proponents argue, a flexible and cost-effective approach to enhancing cybersecurity."[57] NIST's goal was to develop a cost-effective framework that would obviate the need to enact cumbersome regulations across a broad swath of the U.S. economy.[58] By doing this, NIST sought to provide a "common language" for firms, agencies, and other institutions to evaluate their cybersecurity and identify opportunities to mitigate risks, while improving communications both within the institution and with outside parties.[59] The Framework attempted to break data security into essential activities, called "Functions," to enable firms to organize their practices around these specific functionalities.[60] The Framework then further breaks down the Functions into "categories" of activities, and then specific "subcategories" of goals for a firm's information security program, with tiers of activities designed to reflect the differing needs of organizations based on their size and sophistication.[61]

Because the Framework is designed with flexibility in mind, it eschews specific requirements in order to be more generally applicable across industries as well as accommodate existing data security practices a firm may already have in place.[62]

The Framework is voluntary, though it includes incentives for government agencies to participate.[63] However, commentators are hopeful that the Framework could serve as a model for similar standards internationally and in the private sector to establish a uniform approach to evaluating information security.[64] While the NIST Framework represents a step in creating a broad, comprehensive framework, it is still limited by its focus on

---

56 NAT'L INST. OF STANDARDS & TECH., FRAMEWORK FOR IMPROVING CRITICAL INFRASTRUCTURE CYBERSECURITY (Feb. 12, 2014) [hereinafter NIST FRAMEWORK], http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf.

57 Scott J. Shackelford & Andrew Proia, *Why Ignoring the NIST Framework Could Cost You*, HUFFINGTON POST (May 2, 2014), http://www.huffingtonpost.com/scott-j-shackelford/why-ignoring-the-nist-fra_b_5244112.html.

58 Shackelford et al., *supra* note 48, at 309.

59 NIST FRAMEWORK, *supra* note 56, at 1.

60 These functions are Identify, Protect, Detect, Respond, and Recover. NIST FRAMEWORK, *supra* note 56, at 7–9.

61 Shackelford et al., *supra* note 48, at 331–32.

62 *Id.* at 336.

63 Exec. Order No. 13,636, Improving Critical Cybersecurity Infrastructure, 78 Fed. Reg. 11,739, 11,742–43 (Feb. 19, 2013).

64 Shackelford et al., *supra* note 48, at 339–40.

creating and categorizing data security programs, as opposed to setting requirements or articulating a minimum standard of care for handling consumer data.

Both the PCI and NIST standards bring a different approach to the problem of data security, and could function as a baseline for a reasonable data security plan if they were widely adopted. However, the fragmented nature of our current data security regime prevents the industry from relying on any broadly accepted framework, due to the variety of enforcement mechanisms, standards, and statutes to which they are subject.[65] The following section examines this patchwork data security regime and its effects.

B. *The Current Data Security Regime*

With no universal standard or framework for data security, courts, federal regulators, and state governments have each adopted a different approach to enforcing a standard of care for negligent data practices and promoting higher standards of security for consumer data.[66] This patchwork of civil actions, statutory mandates, and regulatory enforcement actions has created a number of overlapping standards that companies must comply with to avoid potential liability.[67] This section examines the current data security regime and how various local, state, and federal authorities attempt to hold companies liable in the event of a negligent data breach.

1. Enforcement by the Courts

In recent years, courts have become more willing to impose liability on firms that allow hackers to compromise consumer data.[68] Tort law is the primary vehicle to impose this liability, normally through class action proceedings.[69] Despite this recent growth in court cases around data security, consumers seeking redress in the court system face high barriers to recovery. Courts have at times held that privacy policies govern data breaches as a contract, and thus limit potential recovery by consumers.[70] Other decisions recognize a tort duty of confidentiality for data holders, while some scholars argue for the creation of an independent tort for "negligent enablement of cybercrime."[71] Proponents of such an independent tort believe it could

---

65 *See infra* Section I.B.

66 *See infra* Section I.B.1-4.

67 *See, e.g.*, Shackelford et al., *supra* note 48, at 312. *See also infra* Section I.B.1-4.

68 Shackelford et al., *supra* note 48, at 312.

69 *See generally* Rustad & Koenig, *supra* note 48.

70 *See, e.g.*, *In re* Sony Gaming Networks & Customer Data Sec. Breach Litig., 903 F. Supp. 2d 942, 961 (S.D. Cal. 2012).

71 Rustad & Koenig, *supra* note 48, at 1557.

help to pierce the liability shields companies create by using mass license agreements that users accept via a checkbox, usually without having read the underlying agreement.[72]

Without a reliable standard of care in common law for data security, and with plaintiffs frequently finding it difficult to prove tangible harm stemming from a privacy violation, courts frequently look to statutes to determine what standard of care is appropriate to impose on companies.[73] This has led to even more scattered judicial holdings, as the number of statutes governing data security continues to multiply.[74] The next section examines the current landscape of statutes governing data breach notification and prevention.

2. Federal Statutes

The federal government has pursued a patchwork of statutory solutions to the problem of securing consumer data, typically as part of larger regulatory schemes focused on particular industries.[75] The result is that a company may face different standards of care and potential liability concerns depending on the industry it operates in.[76] In addition, the FTC now uses its Section 5 authority to pursue enforcement actions across industries,[77] and these actions are frequently informed by the standards laid out in industry-specific federal statutes.[78] Thus, it is instructive to look at the primary federal statutes governing data security in specific contexts before examining how the FTC has taken on its role of filling in the gaps left by these statutory schemes.

---

72 *See id.*, at 1562–63, 1566.

73 *See* Shackelford et al., *supra* note 48, at 314.

74 *Id.* at 324–25.

75 *See* DANIEL J. SOLOVE & PAUL M. SCHWARTZ, PRIVACY, INFORMATION, AND TECHNOLOGY 36–37 (2d ed. 2009) (providing a list of statutes passed by Congress since the 1970's to regulate consumer privacy and data security).

76 *See* Shackelford et. al., *supra* note 48, at 320–24 (summarizing the separate federal statutory schemes in the financial, chemical, healthcare, and energy sectors).

77 15 U.S.C. § 45 (2012) (prohibiting "unfair or deceptive acts or practices in or affecting commerce").

78 *See, e.g.*, FTC *v. Wyndham Worldwide Corp.*, 10 F. Supp. 3d. 602, 615 (D.N.J. 2014) (holding for the first time in federal court that the FTC has authority under Section 5 of the Federal Trade Commission Act to enforce the prohibition against unfair and deceptive acts or practices in the field of data security).

a. *The Financial Context: The Gramm-Leach-Bliley Financial Modernization Act*

Congress adopted the Gramm-Leach-Bliley Act in 1999 to implement a number of reforms to how the financial industry was regulated.[79] This Act revised several financial regulations and established new provisions that governed the collection and use of consumer financial data.[80]

The Act included a Safeguards Rule, which identifies standards for safeguarding customer information by financial institutions that are regulated by the FTC.[81] This Safeguards Rule provided an early framework for how the FTC would enforce data security standards on regulated companies.[82] While the Gramm-Leach-Bliley requirements only govern financial institutions,[83] the FTC has used a similar framework when pursuing action against companies in other industries under its Section 5 authority.[84]

The Safeguards Rule requires a company to develop a written plan for a comprehensive information security program that is appropriate to the company's size and complexity, as well as the sensitivity of the information it collects.[85] The Rule outlines specific objectives as well as required elements for the information security plan.[86] These include designating an employee to coordinate the program, identifying reasonably foreseeable internal and external security risks, and assessing the sufficiency of existing safeguards in light of these identified risks.[87] The institution must take affirmative steps to control the identified risks, regularly monitor and test the effectiveness of its safeguards, and require its vendors by contract to main-

---

79 Gramm-Leach-Bliley Act, Pub. L. No. 106–102, 113 Stat. 1338 (1999) (codified as amended in scattered sections of 12 and 15 U.S.C (2012)).

80 *See generally id*. *See, e.g.*, 15 U.S.C. § 6801 (2012) (declaring that financial institutions are obliged to protect the privacy of its customers).

81 FTC Standards for Safeguarding Consumer Information, 16 C.F.R. §§ 314.1-314.5 (2016). *See also* ANDREW B. SERWIN ET AL., PRIVACY, SECURITY AND INFORMATION MANAGEMENT: AN OVERVIEW 257 (2011).

82 The framework requires appropriate safeguards by financial institutions based on size, complexity, and nature and scope of activities, and sensitivity of customer records. These safeguards must be "reasonably designed" to protect customer information against "anticipated threats or hazards" and "unauthorized access to or use of such information that could result in substantial harm or inconvenience to any customer." 16 C.F.R. § 314.3 (2016). The rule also requires these institutions to "[i]dentify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information." 16 C.F.R. § 314.4 (2016).

83 16 C.F.R. § 314.1(a) (2016) ("[Part 314] implements sections 501 and 505(b)(2) of the Gramm-Leach-Bliley Act, [and] . . . applies to . . . all financial institutions over which the Federal Trade Commission . . . has jurisdiction.").

84 *See* SERWIN ET AL., *supra* note 81, at 257.

85 *Id.* at 257-58.

86 *Id.* at 258-59.

87 16 C.F.R. § 314.4(a)–(b).

tain equivalent safeguards.[88] Finally, the financial institution must regularly adjust its safeguards in light of the required testing.[89] Each of these requirements emphasizes process over any specific technical or functional standard, and each maps very closely to the information security program requirements that make up the core of FTC consent decrees in data security enforcement actions.[90]

b. *The Health Context: Health Insurance Portability and Accountability Act ("HIPAA")*

The Health Insurance Portability and Accountability Act ("HIPAA"),[91] passed in 1996, was designed to create security standards for consumer health data in light of the rise of digital recordkeeping.[92] HIPAA tasks health care entities with protecting "individually identifiable health information" through a set of national standards.[93] The key agency responsible for adopting and implementing these national standards for electronic health information is the Department of Health and Human Services, which published its standards as the HIPAA Security Rule in 2003.[94] The Security Rule covers all individually identifiable health information, and includes administrative, physical, and technical safeguards with which health providers must comply when storing data.[95]

The Security Rule's technical safeguards do not mandate the use of specific technology, and instead require a regulated organization to implement access controls, audit controls, integrity controls, and transmission security measures to protect data.[96] The technical safeguards in the Security Rule are functional, technologically neutral, and provide both a standard by which a regulated entity is measured and implementation specifications to meet that standard.[97] These implementation specifications identify types of functionality that a regulated entity must have in order to comply with the

---

88 16 C.F.R. § 314.4(c)-(d) (2016).

89 16 C.F.R. § 314.4(e) (2016).

90 *See* discussion *infra* Section II.C regarding specific FTC consent decree requirements.

91 Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, 110 Stat. 1936 (1996) (codified as amended in scattered sections of 29 & 42 U.S.C.).

92 *Id.* § 262 (codified as 42. U.S.C. § 1320d-2 (2012)).

93 ERIC A. FISCHER, CONG. RESEARCH SERV., FEDERAL LAWS RELATING TO CYBERSECURITY: OVERVIEW AND DISCUSSION OF PROPOSED REVISIONS 58 (2013).

94 *The Security Rule*, HHS (noting that the Security Rule is located in 45 C.F.R. §§ 160, 164), www.hhs.gov/hipaa/for-professionals/security/ (last visited June 27, 2016); 45 C.F.R. § 160 (2016) ("General Administrative Requirements"); 45 C.F.R. § 164 (2016) ("Security and Privacy").

95 45 C.F.R. § 164 (2016). *See also Summary of the HIPAA Security Rule*, HHS, http://www.hhs.gov/hipaa/for-professionals/security/laws-regulations/index.html (last visited Jan. 7, 2016).

96 45 C.F.R. § 164.312 (a)-(c), (e) (2016).

97 *See id.*

standard, such as a system of unique user identification, a procedure for emergency access to user accounts by administrators, and the use of encryption and decryption for electronic protected health information for the "access control" standard.[98] Under the standard, health entities that fail to protect electronic health data are subject to civil penalties.[99] While HIPAA does not create a private cause of action, some courts have used HIPAA violations as an indication of negligence for private tort suits.[100]

c. *The Web Context: Children's Online Privacy Protection Act ("COPPA")*

Congress passed the Children's Online Privacy Protection Act ("COPPA") in 1998 to regulate how companies collect and use information provided by children online.[101] COPPA applies to any website that is marketed to children or knowingly collects information from children under 13.[102] COPPA contains notice requirements, stipulates that parents must consent to having children's data collected, and allows parents to restrict how their children's data is used once the website collects it.[103] Further, COPPA authorizes the FTC to penalize violations under its Section 5 "unfair and deceptive act or practice" authority, and it denies any private cause of action for harms covered by COPPA.[104]

The FTC has pursued numerous enforcement actions against companies for violating COPPA, and it has been criticized as "among the most paternalistic and authoritarian of the federal privacy statutes thus far" due to its imposition of requirements on parents and prohibition of voluntary disclosures when parents may be indifferent to potential privacy harms.[105] Additionally, some critics have argued that the parental consent requirements of COPPA are too onerous for small websites to comply with, forcing many restrict access to children and self-censor rather than implement a consent program.[106]

---

98 *Id.*

99 42 U.S.C. § 1320d-5 (a)(1)–(2) (2012).

100 Cory J. Fox, *HIPAA Violation Results In $1.44M Jury Verdict Against Walgreens*, *Pharmacist,* BAKER HOSTETLER: HEALTH L. UPDATE (Aug. 22, 2013), http://www.bakerlaw.com/health-law-update-august-22-2013/#HIPAA.

101 Children's Online Privacy Protection Act of 1998, Pub. L. No. 105-277, 112 Stat. 2681-728 (codified as 15 U.S.C. §§ 6501–6506).

102 15 U.S.C. § 6502(a)(1) (2012).

103 *Id.* § 6502(b).

104 15 U.S.C. §§ 57a(a)(1)(B), (e)(5)(C) (2012).

105 Anita L. Allen, *Minor Distractions: Children, Privacy and E-Commerce*, 38 HOUS. L. REV. 751, 775–76 (2001).

106 *See* Melanie L. Hersh, Note, *Is COPPA a Cop Out? The Child Online Privacy Protection Act as Proof That Parents, Not Government, Should be Protecting Children's Interests on the Internet*, 28

However, even commentators critical of COPPA praise the law's safe harbor program as "the part of COPPA designed with the most foresight" due to its attempt to give control of compliance to the industry, rather than government.[107] COPPA provides safe harbors for regulated websites, stating that if a website operator "follows self-regulatory guidelines issued by marketing or online industry groups that are approved by the FTC, then the COPPA requirements will be deemed satisfied."[108] Currently, seven programs have been approved as COPPA safe harbors.[109] The COPPA safe harbor program is designed to encourage industry self-regulation by allowing private organizations to create their own oversight programs and file with the Commission to have them approved.[110] Once the Commission approves a program, any business that participates in the program is deemed to have satisfied the standards of COPPA.[111] A business participating in an approved program is then only subject to review and liability under the terms of the program, and is not subject to direct action by the FTC.[112] Thus, the safe harbor allows industry actors to act as a buffer or middleman between individual websites and federal regulators.[113]

While the federal government has passed numerous statutes on data security, it is not the only actor seeking to regulate this space. Nearly every state has passed some form of data security law, creating a patchwork of statutory obligations for companies to navigate. The next section explores these state-level regulations.

3. State Statutes

Today, the vast majority of states have enacted their own laws on data security.[114] Initially, states focused on breach notification, requiring companies to notify their customers in the event their personal information was

---

FORDHAM URB. L.J. 1831, 1865–67 (2001); Joshua Warmund, Note, *Can COPPA Work? An Analysis of the Parental Consent Measures in the Children's Online Privacy Protection Act*, 11 FORDHAM INTELL. PROP., MEDIA & ENT. L.J. 189, 212–15 (2000).

107 Hersh, *supra* note 106, at 1864–65.

108 SOLOVE & SCHWARTZ, *supra* note 75, at 449. *See also* 15 U.S.C. § 6503 (2012).

109 Leslie G. Moylan & Ronald London, *COPPA's "Safe Harbor" Grows with FTC's Approval of iKeepSafe's Self-Regulating Framework,* PRIVACY & SEC. L. BLOG (Aug. 8, 2014), http://www.privsecblog.com/2014/08/articles/technology/coppas-safe-harbor-grows-with-ftcs-approval-of-ikeepsafes-self-regulating-framework/.

110 FTC Safe harbor programs, 16 C.F.R. § 312.11 (2016). *See also COPPA Safe Harbor Program*, FTC, https://www.ftc.gov/safe-harbor-program (last visited Jan. 7, 2016).

111 16 C.F.R. § 312.11(g).

112 *Id*. *See also COPPA Safe Harbor Program*, *supra* note 110.

113 Hersh, *supra* note 106, at 1864–65.

114 *Security Breach Notification Laws*, NAT'L CONF. OF STATE LEGISLATURES (last updated Jan. 4, 2016), http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx.

compromised by a data breach.[115] More recently, states have moved beyond breach notification to codify standards of care and obligations that companies have to secure consumer data.[116] These statutes create a patchwork of frequently overlapping obligations that impose enormous compliance costs on companies seeking to do business in multiple states.[117] This section examines the current landscape and history of state data security regulation.

a. *State Breach Notification Laws*

Currently, 47 states and the District of Columbia have data breach notification laws, requiring companies that are the victims of a breach to notify customers when their personally identifiable information has been compromised.[118] These statutes vary widely in their requirements, and sometimes contradict each other, making compliance difficult for companies operating across state lines.[119]

The first area where these laws vary is the trigger of notification obligations. Most states require that companies notify their customers when they have a "reasonable belief that there has been an unauthorized acquisition of unencrypted data."[120] This obligation typically comes into effect when the company discovers or is notified of the breach.[121] However, there is a great deal of variety in how broadly states define the type of data that is covered by notification statutes. Some states, such as California, require notification for every breach, whereas states with narrower laws, like Florida, only require notification when there is a reasonable likelihood of harm to consumers.[122] While some state laws apply only to unencrypted data, others specify that notification is only required for personally identifiable information or medical information.[123] Form of notice also varies between states, with different states requiring notice by telephone, statewide media, email, or letter to a state consumer protection bureau.[124] Still, there are some areas of commonality between the states, such as the requirement for direct,

---

115 JIM HALPERT & MICHELLE J. ANDERSON, STATE BREACH NOTIFICATION LAWS — UPDATES FROM THE 2015 LEGISLATIVE SESSION, 6 ACTION STEPS FOR COMPANIES 1 (Jul. 20, 2015), https://www.dlapiper.com/en/us/insights/publications/2015/07/state-breach-notification-laws/.

116 *Id.* at 2.

117 Mike Tsikoudakis*, Patchwork of Data Breach Notification Laws Poses Challenge*, BUS. INS. (June 5, 2011), www.businessinsurance.com/article/99999999/NEWS070101/399999961.

118 *Security Breach Notification Laws*, *supra* note 114.

119 Shackelford et al., *supra* note 48, at 324–25; *See also* Tsikoudakis*, supra* note 117.

120 SERWIN ET AL., *supra* note 81, at 285.

121 *See, e.g.*, ALASKA STAT. § 45.48.010 (2015); ARIZ. REV. STAT. ANN. § 44-7501 (2016); CAL. CIV. CODE § 1798.29 (Deering 2016).

122 SERWIN ET AL., *supra* note 81, at 285–86.

123 *Id.*

124 *Id.* at 286.

as opposed to substitute, notice, as well as a recognition that federal law preempts the state statute for certain industries.[125]

The differing requirements of the states' notification statutes mean that a company operating in multiple states must navigate multiple compliance processes, and it may have notification obligations triggered in different states by different events. But due to the potential for large data breaches to become national news and affect stock prices, the impact of a data breach will be felt as soon as the earliest state disclosure requirement takes effect. This means that the states with the most stringent notification regimes effectively set the notification requirements for the rest of the country, though the actual information the company is required to disclose to consumers will still vary by state. As a result, the notification statutes have created a costly patchwork of regulations and procedures that companies must navigate if they become the victims of a breach.

b. *State Breach Prevention Laws*

While the earliest statutes on data security focused on notification, newer, broader state statutes have attempted to enter the breach prevention realm and establish a standard of care for companies in the state.[126] The Massachusetts data breach law, widely considered the broadest of the state breach prevention statutes, requires companies to have a regularly-audited information security plan, not unlike the federal requirements imposed in statutes like Gramm-Leach-Bliley.[127] Other states require only "'reasonable' security measures," while doing little to define the term.[128] Many states do not require the breach to cause any harm to consumers for notification statutes to be triggered, whereas some maintain the harm requirements generally enforced by the courts.[129] Thus, companies that seek to do business and collect data across state lines are met with a constantly shifting and disparate set of statutes, many with a vaguely defined standard of care.[130]

This lack of uniformity in state regulations has created a great deal of uncertainty in the data security regime. As a result, the federal government

---

125 *Id.*

126 HALPERT & ANDERSON, *supra* note 115, at 1–2.

127 *Compare* Shackelford et al., *supra* note 48, at 325, *with* FTC Standards for safeguarding customer information, 16 C.F.R. §§ 314.3-4 (2016).

128 Shackelford et al., *supra* note 48, at 325–26 (footnote omitted).

129 *See generally State Data Breach Law Summary*, BAKER HOSTETLER (describing the notification triggering laws for 51 states and territories), http://www.bakerlaw.com/files/Uploads/Documents/Data%20Breach%20documents/State_Data_Breach_Statute_Form.pdf (last visited Jan. 8, 2016). *See, e.g.*, *id. Colorado* ("when an individual or commercial entity becomes aware of a breach"). *But see id. Delaware* ("when an individual or entity . . . becomes aware" and misuse has occurred or is likely to occur).

130 *See* John Black, *Developments in Data Security Breach Liability*, 69 BUS. LAW. 199, 206 (2013).

has sought to fill the gaps left by the patchwork of state statutes.[131] Over the years, data security regulation on the federal level has gradually become consolidated in the FTC, which is now considered the de facto regulator of privacy harms in the U.S.[132] This authority has grown gradually as the FTC has used its authority to regulate unfair trade practices to penalize companies for perceived consumer harms.[133] The next section analyzes the evolution of the FTC's authority to regulate privacy harms under its Section 5 statutory mandate.

4. FTC Authority

While Congress originally established the FTC in 1914 to promote commercial competition, it later expanded the Commission's authority by amending the FTC Act to allow the Commission to regulate not just competition between companies, but practices that were "unfair or deceptive" to consumers.[134] Initially, the FTC used this authority to police violations of antitrust and consumer protection laws, but beginning in 1995, the Commission began to use its authority to police consumer privacy harms.[135]

Today, the FTC is the lead regulator of the privacy and data security practices of private companies.[136] Section 5 of the FTC Act is the principle source of authority the agency uses to pursue enforcement actions against companies that are victims of data breaches.[137] Section 5 of the Act establishes two prongs by which the FTC may penalize companies: one for "deceptive" practices and one for "unfair" practices.[138] While the deceptive practices prong is still used by the Commission in privacy and data security actions, the "unfairness prong" has now become the primary vehicle by which the FTC enforces data security standards.[139] In the FTC's early actions to police privacy harms, it penalized companies for actions that used consumer data in violation of a company's posted privacy policy, charging

---

131 Daniel J. Solove & Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, 114 COLUM. L. REV. 583, 586–87 (2014).

132 *Id.* at 588, 590.

133 *Id.* at 599.

134 *Id*. at 598.

135 FED. TRADE COMM'N, PRIVACY ONLINE: FAIR INFORMATION PRACTICES IN THE ELECTRONIC MARKETPLACE: A REPORT TO CONGRESS 3 (May 2000), https://www.ftc.gov/reports/privacy-online-fair-information-practices-electronic-marketplace-federal-trade-commission. *See also* Solove & Hartzog, *supra* note 131, at 598.

136 Solove & Hartzog, *supra* note 131, at 590.

137 FED. TRADE COMM'N, *Privacy & Data Sec. Update (2014)* (Jan. 2015), https://www.ftc.gov/reports/privacy-data-security-update-2014.

138 15 U.S.C. § 45(a)(1) (2012).

139 *See, e.g.*, FTC v. Wyndham Worldwide Corp., 799 F.3d 236, 240 (3d Cir. 2015); Complaint at 5, *In re* LabMD, Inc., No. 9357 (F.T.C. Aug. 28. 2013).

companies with making misrepresentations about their data collection or data usage practices under the "deceptive practices" prong.[140]

The FTC's sole reliance on the "deceptive practices" prong limited its effectiveness in enforcing privacy harms, because many consumers simply ignore or do not read posted privacy policies.[141] Today, however, the Commission examines the totality of the representations a company makes, including its marketing and the design of its website, to determine whether the company made a misrepresentation about its privacy or security practices.[142] This examination is not limited to the initial data collection, but any use of data after it is collected that is inconsistent with the context within which the company originally collected it.[143] The FTC has used this prong to penalize companies that misrepresent the level of security they use to protect consumer data, whether intentionally or negligently.[144]

While the "deceptive practices" prong allowed the FTC to take action against some data security harms, it restricted the Commission to taking action in situations where a company had made an affirmative representation about the level of security it provided, leaving the Commission unable to enforce minimal security standards if no representation was made.[145] To overcome this limitation, the FTC now relies on the "unfairness" prong of

---

140 Press Release, FED. TRADE COMM'N, Internet Site Agrees to Settle FTC Charges of Deceptively Collecting Personal Information in Agency's First Internet Privacy Case (Aug. 13, 1998), https://www.ftc.gov/news-events/press-releases/1998/08/internet-site-agrees-settle-ftc-charges-deceptively-collecting.

141 *See, e.g.*, Courteney Palis, *Facebook Privacy Options Ignored by Millions of Users: Consumer Reports*, HUFFINGTON POST (May 3, 2012) (noting 13 million Facebook users were unaware of or did not use the network's privacy control settings), http://www.huffingtonpost.com/2012/05/03/facebook-privacy-consumer-reports_n_1473920.html.

142 *See, e.g., In re* Snapchat, Inc., No. C-4501, 2014 WL 7495798, at *7–8 (F.T.C. Dec. 23, 2014); *In re* GMR Transcription Servs, Inc., No. C-4502, 2014 WL 4252393, at *6 (F.T.C. Aug. 14, 2014); *In re* Fandango, LLC, No. C-4481, 2014 WL 4252396, at *6–7 (F.T.C. Aug. 13, 2014); *In re* Credit Karma, Inc., No. C-4480, 2014 WL 4252397, at *6–7 (F.T.C. Aug. 13, 2014).

143 *See, e.g.*, *In re Snapchat*, 2014 WL 7495798, at *7; *In re Fandango*, 2014 WL 4252396, at *6; *In re Credit Karma*, 2014 WL 4252397, at *6.

144 An intentional privacy harm could include a deliberate misrepresentation, such as collecting more data than a consumer consented to provide without the consumer's knowledge. *See, e.g., In re Snapchat*, 2014 WL 7495798, at *3–4 (counts 1-5). A negligent harm can also be penalized under the misrepresentation prong if the FTC determines that a company misrepresented its actual level of data security to consumers and user data was later breached. *See, e.g.*, *In re GMR Transcription Servs*, 2014 WL 4252393, at *4 (failure to take "reasonable and appropriate" measures); *In re Fandango*, 2014 WL 4252396, at *4 (failure to provide "reasonable and appropriate . . . security"); *In re Credit Karma*, 2014 WL 4252397, at *4 (failure to use "reasonable and appropriate security practices").

145 The deceptive practices cases contain findings that the defendant represented certain data privacy or security claims, expressly or by implication. *See, e.g.*, *In re Snapchat*, 2014 WL 7495798, at *3–5, 6 ("represented, expressly or by implication"); *In re GMR Transcription Servs*, 2014 WL 4252393, at *4 ("represented, expressly or by implication"); *In re Fandango*, 2014 WL 4252396, at *4 ("represented, expressly or by implication"); *In re Credit Karma*, 2014 WL 4252397, at *4–5 ("represented, expressly or by implication"). *See also* Solove & Hartzog, *supra* note 131, at 599.

its authority to take action against companies that have negligent data security practices but may not make specific representations about their level of security.[146] Under this authority, the FTC no longer needs to prove a misrepresentation was made to impose liability, and can instead rely on a standard of "reasonable and appropriate" data security practices.[147] The FTC argues that a failure to maintain reasonable and appropriate data security is a practice that is presumptively unfair to consumers.[148] This more nebulous authority has given the FTC much greater leeway to pursue action against companies that suffer data breaches than it would have relying on the more concrete "deceptive practices" prong.[149]

In recent years, the FTC steadily increased the number of privacy and data security violations it pursued, totaling at least 50 actions against companies for unreasonable data security practices.[150] To date, there have been very few court challenges to the FTC's authority, and the FTC has issued little specific guidance on the standards by which it judges a company's data security.[151]

II. THE IMPACT OF FTC ENFORCEMENT

With no official federal arbiter of online data practices, the FTC has gradually used its statutory authority to become the de facto regulatory watchdog for data security breaches.[152] However, the FTC's authority is murky at best, as it has not been thoroughly examined by courts, with most actions brought by the FTC ending in settlements as opposed to litigation.[153]

---

146 *See, e.g.*, FTC v. Wyndham *Worldwide Corp.*, 799 F.3d 236, 240 (3d Cir. 2015) (alleging that unreasonable cybersecurity practices were "unfair"); *In re GMR Transcription Servs*, 2014 WL 4252393, at *4 (finding that the failure "to employ reasonable and appropriate measures . . . was . . . an unfair act."). *See also* Solove & Hartzog, *supra* note 131, at 599.

147 *See Wyndham* Worldwide Corp., 799 F.3d at 240 (unreasonable cybersecurity practices "unfair"); *In re GMR Transcription Servs*, 2014 WL 4252393, at *4 (finding that the failure "to employ reasonable and appropriate measures . . . was . . . an unfair act"); *In re Fandango*, 2014 WL 4252396, at *4 (representations "unfair or deceptive"); *In re Credit Karma*, 2014 WL 4252397, at *5 (representations "unfair or deceptive"). *See also* Solove & Hartzog, *supra* note 131, at 599.

148 *See, e.g.*, *Wyndham* Worldwide Corp., 799 F.3d 236, 240 (3d Cir. 2015) (unreasonable cybersecurity practices "unfair"); *In re GMR Transcription Servs*, 2014 WL 4252393, at *4 (finding that the failure "to employ reasonable and appropriate measures . . . was . . . an unfair act").142

149 *See* Solove & Hartzog, *supra* note 131, at 599.

150 FED. TRADE COMM'N, START WITH SECURITY: A GUIDE FOR BUSINESS (June 2015), https://www.ftc.gov/tips-advice/business-center/guidance/start-security-guide-business.

151 *See* Solove & Hertzog, *supra* note 131, at 588; Donald G. Aplin, *The Lone Man to Challenge an FTC Data Security Enforcement Action*, BLOOMBERG BNA: PRIVACY & DATA SEC. BLOG (Apr. 29, 2016), http://www.bna.com/lone-man-challenge-b57982070501/.

152 Ryan T. Bergseiker et al., *The Federal Trade Commission's Enforcement of Data Security Standards*, 44 COLO. LAW. 39, 39 (June 2015).

153 *See* Solove & Hertzog, *supra* note 131, at 588.

Recently, courts have begun to weigh in on the FTC's authority, but their decisions have only made it more difficult for companies to determine what they must do to comply with the FTC's data protection standards, lest they be sanctioned for failure to maintain a reasonable data security program.[154] This section will examine the FTC's enforcement actions, guidance, and the recent court decisions that have attempted to shed light on the standards the FTC seeks to enforce.

A. Wyndham *and the Third Circuit's View of FTC Authority*

Until recently, the courts were silent on the FTC's use of Section 5 authority to police data security practices. Of the over 50 enforcement actions taken by the FTC against companies for unfair or deceptive data security practices, the vast majority ended in consent decrees.[155] Because of the dearth of litigation, the FTC was operating in a legal gray area, with no official sanction for its expanding role as the nation's data security watchdog.[156] This status was recently solidified by the Third Circuit's decision in *FTC v. Wyndham Worldwide Corp.*[157] This section analyzes the recent *Wyndham* decision, and examines the court's reasoning and the potential impact on other corporations from this broad confirmation of FTC authority.

In *Wyndham*, the FTC filed suit against the global hospitality company after alleged data security failures led to three data breaches in two years at hotels owned by Wyndham and its subsidiaries, alleging that Wyndham's security practices enabled the theft of personal data and credit card information of 619,000 customers, with a resulting $10.6 million in losses to consumers.[158] Wyndham challenged the FTC's authority to undertake an enforcement action under Section 5, arguing that negligent data security could not constitute an unfair practice, and that the FTC had not provided fair notice of the type of conduct that would fall below the required standard of care for data security.[159]

The Third Circuit found in favor of the FTC, rejecting Wyndham's arguments.[160] The court held that the hotel chain's due process concerns and

---

154 *See id.* at 612–614 (explaining that Section 5 violations rarely go to court, where companies face greater risk of monetary sanctions and reputational damage than in settlements).

155 *Id.* at 585; FED. TRADE COMM'N, START WITH SECURITY, *supra* note 150.

156 *See* Solove & Hertzog, *supra* note 131, at 585–86 (describing the FTC's privacy jurisprudence as "common law").

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

158 Complaint for Injunctive and Other Equitable Relief at 2, 17, FTC v. Wyndham Worldwide Corp., 10 F. Supp. 3d 602 (D.N.J. 2012) (No. 2:13-CV-01887); *Wyndham Worldwide Corp.*, 799 F.3d at 242.

159 *Wyndham Worldwide Corp.*, 799 F.3d at 244, 249.

160 *Id.* at 259.

lack of notice arguments were unpersuasive, because Wyndham had adequate notice of the meaning of the FTC's statute, which used ordinary tort negligence principles.[161] Thus, Wyndham was not entitled to know the FTC's specific interpretation of the statute, nor was the FTC required to propagate specific guidelines for data security procedures.[162] The court instead held that existing FTC guidance, the FTC's complaint itself, and the fact that Wyndham's actions did not match those held out in its privacy policy demonstrated that Wyndham had adequate notice of what constituted a reasonable data security program and thus could be held liable for the breach.[163]

The court also affirmed that the FTC has the statutory right to enforce privacy and data security obligations on companies, thus solidifying the FTC's role as the primary regulatory watchdog in the data security space.[164] Specifically, the *Wyndham* court reasoned that under the FTC statute, an act need not be "unscrupulous" or "unethical" to qualify as "unfair" under the statute.[165] The court further held that the FTC was not precluded from regulating privacy and data security when there were other federal statutes that also regulated this area, and it held that Wyndham could be held to have acted unfairly despite itself being the victim of the same crime as its customers.[166]

A company seeking to avoid a similar fate can take away several lessons from this decision. It seems clear now that the FTC has the authority to enforce data security standards and is likely to increase its action in this area in the future.[167] Additionally, the court's holding that the presence of other data breach statutes did not preclude broad powers for the FTC in this area may encourage other agencies, such as the FCC, to begin regulating data security more aggressively themselves.[168] For example, the FCC has

---

161 *See id.* at 253–54.

162 *See id.* at 255–56.

163 *Id.* at 256–57.

164 *See id.* at 248.

165 FTC v. Wyndham Worldwide Corp., 79 F.3d 236, 244 (3d. Cir. 2015).

166 *Id.* at 246, 248.

167 *Id.* at 246–249 (rejecting that Wyndham's "conduct falls outside the plain meaning of [15 U.S.C. § 45(a)]" and finding that "unfairness actions [resulting from] inadequate cybersecurity . . . [are] not inconsistent with the [FTC's] earlier position").

168 The FCC, under authority given to it by the recent Open Internet proceeding's reclassification of broadband as a Title II Common Carrier service, has recently begun fining major cable companies and telecommunications carriers for being victimized by hackers. *See, e.g.*, Brian Fung, *In a First, the FCC is Fining a Major Cable Company for Getting Hacked*, WASH. POST (Nov. 5, 2015), https://www.washingtonpost.com/news/the-switch/wp/2015/11/05/cox-to-pay-nearly-600000-to-the-fcc-after-getting-hacked-by-lizard-squad/; Brian Fung, *AT&T Will Pay $25 Million After Call-Center Workers Sold Customer Data*, WASH. POST (Apr. 8, 2015), https://www.washingtonpost.com/news/the-switch/wp/2015/04/08/att-will-pay-25-million-after-call-center-workers-sold-customer-data/; Brian Fung, *With a $10 Million Fine, the FCC is Leaping Into Data Security for the First Time*, WASH. POST (Oct. 24, 2014), https://www.washingtonpost.com/news/the-switch/wp/2014/10/24/with-a-10-million-

already begun rulemaking procedures in an attempt to codify new privacy and data security obligations stemming from the reclassification of broadband as a Title II common carrier in the 2015 Open Internet Order.[169] Because the Third Circuit affirmed that the FTC is under no obligation to issue specific guidance or standards before bringing an action, it is increasingly unlikely that the agency will constrain its authority by doing so, meaning that companies will be left to examine past FTC enforcements to determine whether their practices are adequate.[170] The following sections look at these enforcement actions and published guidance to determine what practices the FTC looks to when deciding to file a complaint against a company.

B. *FTC Enforcement and Guidance*

While the FTC has not issued a large number of consent decrees on data security issues, the number of actions the FTC takes in this area is increasing,[171] and there are some lessons that can be gleaned from both the FTC's complaints and consent decrees. This section will analyze the FTC's enforcement actions and consent decrees to determine what types of violations the Commission feels are actionable under its Section 5 authority, as well as what standards the Commission seeks to enforce when it enters into a consent decree with a company. It will also examine published FTC guidance and statements on data security to determine whether a clear standard of care can be gleaned from existing FTC actions.

The FTC has pursued over 50 enforcement actions since 2002 for data security violations under its Section 5 authority.[172] The conduct by companies that can trigger an enforcement action varies greatly, though most

---

fine-the-fcc-is-leaping-into-data-security-for-the-first-time/. The Commission has stated that its authority only extends to carriers, rejecting a petition requesting that it regulate the data collection and privacy practices of "edge providers" like Google and Facebook. *In re* Consumer Watchdog Petition for Rulemaking to Require Edge Providers to Honor 'Do Not Track' Requests, 30 FCC Rcd. 12424, 12424 (2015) ("The [FCC] has been unequivocal in declaring that it has no intent to regulate edge providers."); Brian Fung & Andrea Peterson, *The FCC Says It Can't Force Google and Facebook to Stop Tracking Their Users*, WASH. POST (Nov. 6, 2015), https://www.washingtonpost.com/news/the-switch/wp/2015/11/06/the-fcc-says-it-cant-force-google-and-facebook-to-stop-tracking-their-users/.

169 Elizabeth Drogula & Christin McMeley, *FCC to Initiate Privacy Rulemaking in "Autumn"*, OPEN INTERNET L. ADVISOR (June 30, 2015), http://www.openinternetlaw.com/2015/06/fcc-to-initiate-privacy-rulemaking-in-autumn/.

170 *Wyndham Worldwide Corp.*, 799 F.3d at 253–55 (holding that "Wyndham was not entitled to know with ascertainable certainty the FTC's interpretation of what cybersecurity practices are required by [15 U.S.C.] § 45(a).").

171 *See* FED. TRADE COMM'N, PRIVACY & DATA SEC. UPDATE: 2015, *supra* note 4, at 2, 4 (fewer than 60 data security cases since 2002).

172 *Id.*

complaints contain both a misrepresentation and an unfair practices count, utilizing each prong of Section 5.[173]

In a complaint against GMR Transcription Services, Inc., a provider of medical transcription services, the FTC alleged an unfair practices violation against the company for its failure to confirm that employees had installed antivirus software and for its failure to ensure, either by contract or monitoring, that its service provider used appropriate security measures.[174] GMR allowed sensitive personally identifiable health data to be indexed by search engines, though the FTC did not allege a specific causal connection between the inadequate security procedures and the alleged harm of exposing medical records, nor did the Commission allege specific damages to consumers.[175]

In another medical data case against Accretive Health, Inc., the FTC alleged that the company's failure to secure laptops against theft, restrict access by employees to sensitive consumer data, and ensure that employees properly removed information from computers was a failure to employ reasonable and appropriate measures that constituted an unfair practice.[176] Here, the FTC did not name a specific technical failure in its complaint, but instead focused on administrative safeguards and policies on data and technology use by employees.[177] Similarly, in its complaint against TRENDnet, Inc., the Commission focused on the company's failure to properly secure login credentials for its IP camera software, and further noted the company's failure to implement a process to monitor for security vulnerabilities in its system.[178]

In contrast with these complaints, which largely focused on security process failures, the FTC's complaint against HTC America, Inc. focused on specific technical failures by the company, which led to vulnerabilities.[179] The complaint outlines four technical practices that constituted a failure to implement reasonable and appropriate security procedures.[180] These failures include the introduction of "permission re-delegation" vulnerabilities by failing to use accepted industry security practices, preinstalling a custom application on to consumer's devices that circumvented the normal installation process, failing to use secure logging applications, and failing to deactivate "debug" code once devices were shipped.[181] For

---

173 *See, e.g.*, *In re* GMR Transcription Servs, Inc., No. C-4502, 2014 WL 4252393, at *4 (F.T.C. Aug. 14, 2014); *In re* Trendnet, Inc., No. C-4426, 2014 WL 556262, at *4 (F.T.C. Jan. 16, 2014); *In re* HTC Am., Inc., No. C-4406, 2013 WL 3477025, at *7 (F.T.C. June 25, 2013).

174 *In re GMR Transcription Servs*, 2014 WL 4252393, at *3–4.

175 *See id.*

176 *In re* Accretive Health, Inc., No. C-4432, 2014 WL 726603, at *1–2 (F.T.C. Feb. 5, 2014).

177 *Id.*

178 *In re Trendnet*, 2014 WL 556262, at *2–3.173

179 *In re HTC Am.*, 2013 WL 3477025, at *1–5.

180 *Id.* At *2–5.

181 *Id.*

each of these failures, the FTC emphasized that there were widely available, industry-standard fixes that could have alleviated these vulnerabilities, but which were ignored by HTC.[182]

This represents a key factor in how the FTC evaluates security vulnerabilities, as the FTC appears far more likely to penalize specific technical failures if fixes are widely available or known in the industry and are not cost-prohibitive compared to the potential harm to consumers.[183] Thus, the FTC appears to expect companies to perform a cost-benefit analysis when designing its security program, with the level of expected safeguards scaling with the potential harm to consumers if a breach occurs, as well as with the potential cost of the safeguards.

Regardless of whether a company is penalized for process, oversight, or technical failures, once the company decides to settle with the FTC, the consent decree typically includes two main provisions, one targeting misrepresentation under the "deceptive practices" prong, and one targeting inadequate or unreasonable data security under the "unfairness" prong.[184] While the misrepresentation charges typically focus on a fairly straightforward decree to cease all false statements or misrepresentations about privacy and security practices, the unfairness charges typically require that the settling company put a comprehensive information security plan in place with regular processes to monitor its effectiveness and increase accountability.[185]

The requirements of the FTC's settlement-mandated security programs generally mirror those that the Gramm-Leach-Bliley Act requires of financial institutions, and focus on instituting processes and mechanisms to ensure regular audits of a documented security plan.[186] As such, companies are frequently required to appoint an officer to oversee the data security program, to have a third party conduct a risk assessment, to identify any threats and implement steps to mitigate them, and to conduct regular testing and

---

182 *Id.*

183 Kathryn F. Russo, *Regulation of Companies' Data Security Practices Under the Federal Trade Commission Act and California Unfair Competition Law,* 32 COMPUTER & INTERNET LAW. 14, 14–15 (2015).

184 *See In re* Snapchat, Inc., No. C-4501, 2014 WL 7495798, at *6 (F.T.C. Dec. 23, 2014) (deceptive acts); *In re GMR Transcription Servs*, 2014 WL 4252393, at *4 (deceptive and unfair acts); *In re* Fandango, LLC, No. C-4481, 2014 WL 4252396, at *4 (F.T.C. Aug. 13, 2014) (deceptive or unfair acts); *In re* Credit Karma, Inc., No. C-4480, 2014 WL 4252397, at *5–7 (F.T.C. Aug. 13, 2014) (deceptive or unfair acts).

185 *In re Snapchat*, 2014 WL 7495798, at *7–9; *In re GMR Transcription Servs*, 2014 WL 4252393, at *6–8; *In re Fandango*, 2014 WL 4252396, at *6–7; *In re Credit Karma*, 2014 WL 4252397, at *6–8.

186 *Compare In re Snapchat*, 2014 WL 7495798, at *7-9, *In re GMR Transcription Servs*, 2014 WL 4252393, at *6–8, *In re Fandango*, 2014 WL 4252396, at *6–7, *and In re Credit Karma*, 2014 WL 4252397, at *6–8, *with* Gramm-Leach-Bliley Act, Pub. L. No. 106–102, § 501, 113 Stat. 1338, 1436–38 (1999).

audits to assess effectiveness and identify new vulnerabilities.[187] These requirements do not vary according to the type of violation, whether a technical, administrative, or physical failure.[188] Even when the FTC specifically names technical failures in its complaints, as in the HTC proceeding, it refrains from mandating any technical changes, instead continuing to focus on process and administrative oversight.[189]

However, these recommended procedures still leave gaps for companies seeking to provide adequate security, as there is no indication of what threats could bring about charges of negligent practices, or what level of risk mitigation is required for a company's practices to be deemed reasonable. Instead, the typical FTC complaint comes after a vulnerability has been discovered, whether it be technical or physical, and focuses on process failures at a company that prevented the identification or remediation of the vulnerability.[190] The FTC typically focuses on functional, standards-based guidance as opposed to specific technical requirements for what constitutes reasonable and unreasonable data security measures.[191] In recent actions, the FTC has focused its evaluation of the targeted company's data security on the sensitivity of the data compromised, the method that was used to expose the data, and the relative cost and availability to methods to prevent the breach when compared to the potential harm of a breach.[192] This approach increases flexibility for the FTC to pursue actions against companies that suffer breaches, but it seems that the only surefire indication that a company's security program is inadequate is if that company is eventually hacked.

While the Third Circuit ruled in favor of broad FTC authority in *Wyndham*, challenges to this authority could arise in other circuits, such as in the ongoing litigation of the FTC's enforcement action against

---

187 *See, e.g.*, *In re Snapchat*, 2014 WL 7495798, at *8; *In re GMR Transcription Servs*, 2014 WL 4252393, at *6; *In re Fandango*, 2014 WL 4252396, at *6–7; *In re Credit Karma*, 2014 WL 4252397, at *7. *See also* Google, Inc.: Analysis of Proposed Consent Order to Aid Public Comment, 76 Fed. Reg. 18,762, 18,763-64 (Apr. 5, 2011).

188 *See In re Snapchat*, 2014 WL 7495798, at *5-8 (technical violation); *In re GMR Transcription Servs*, 2014 WL 4252393, at *3, 6 (technical and administrative violations); *In re Accretive Health*, 2014 WL 726603, at *1–4 (physical, technical, and administrative violations); *In re Trendnet*, 2014 WL 556262, at *2-3, 7-8 (technical and administrative violations).

189 *See In re HTC Am.*, 2013 WL 3477025, at *1–5, 9–11.

190 *E.g.*, *In re GMR Transcription Servs*, 2014 WL 4252393, at *3; *In re HTC Am.*, 2013 WL 3477025, at *1–6.

191 *See generally* FED. TRADE COMM'N, START WITH SECURITY, *supra* note 150; *Prepared Statement of the Federal Trade Commission on Data Security*: *Hearing Before the H. Comm. on Energy & Commerce*, 112th Cong. 7–8 (2011) (statement of Edith Ramirez, Comm'r, FTC), https://www.ftc.gov/sites/default/files/documents/public_statements/prepared-statement-federal-trade-commission-data-security/110615datasecurityhouse.pdf.

192 *See, e.g.*, FTC v. Wyndham Worldwide Corp., 799 F.3d 236, 241–42, 256 (3d Cir. 2015); Complaint at 3, *In re* LabMD, Inc., No. 9357 (F.T.C. Aug. 28. 2013).

LabMD.[193] LabMD, a medical testing company accused of exposing consumer medial data in two separate events, has challenged the FTC's statutory authority, as well as its reliance on testimony from a third-party data vendor through which the Commission sought to hold LabMD liable.[194] However, the rising crisis in data security confirms that we now live in an age where for most companies, it may only be a matter of time before their data is breached or stolen, no matter the precautions they take. The apparent inevitability of successful cyber attacks makes discerning a standard of care even more important for bodies seeking to regulate data security while only punishing those companies that have truly been negligent in their handling of consumer data.

C. *What is the Standard of Care for Data?*

While the Third Circuit has held that the FTC does not have a duty to propagate specific regulations prior to an enforcement action,[195] the combination of consent decrees and guidance for businesses provided by the FTC can give a sense of what standard of care the FTC will actually enforce.[196] The FTC's actions indicate that there is an expected minimum level of security required of most companies, but the FTC's guidance does not do enough to provide clear standards for how a business needs to behave in order to avoid potential liability and sanctions from the agency.[197] This section analyzes what lessons companies can take from the current data security regime, and whether they are adequate to raise the standard of care for data while ensuring that only negligent companies are punished when their data is breached.

First, the FTC is focused on the context of data collection and retention.[198] The FTC will frequently look to the nature, size, and complexity of the business in question to determine the appropriate level of security to

---

193 LabMD, Inc. v. FTC, 776 F.3d 1275, 1279–80 (11th Cir. 2015) (affirming the trial court's ruling that LabMD's challenge was premature because the administrative process was incomplete). *See also Wyndham Worldwide Corp.*, 799 F.3d at 253–54 (describing the FTC's 15 U.S.C. § 45(a) as flexible, evolving, and left to the FTC for development in affirming the FTC's order against the defendant).

194 *LabMD*, 776 F.3d at 1277. *See also* Marianne Kolbasuk McGee, *Bombshell Testimony in FTC's LabMD Case*, DATA BREACH TODAY (May 8, 2015), http://www.databreachtoday.com/bombshell-testimony-in-ftcs-labmd-case-a-8212. Questions about the FTC's reliance on vendor testimony to implicate LabMD, eventually lead to Congressional scrutiny of the FTC's actions in the case by the House Oversight and Government Reform Committee. Marianne Kolbasuk McGee, *LabMD Case: House Committee Gets Involved*, HEALTHCARE INFO SECURITY (June 12, 2014), http://www.healthcareinfosecurity.com/labmd-case-house-committee-gets-involved-a-6951.

195 *Wyndham Worldwide Corp,* 799 F.3d at 253–55, 259.

196 *See* Solove & Hartzog, *supra* note 131, at 661.

197 *Id.*

198 *See* FED. TRADE COMM'N, START WITH SECURITY, *supra* note 150, at 2.

enforce.[199] Thus, companies that collect large amounts of sensitive data, such as financial institutions and health care providers, can expect a much higher standard of care than businesses that deal with fewer records or do not handle financial or health data.[200] Second, the FTC will look at the context in which data is collected.[201] Use or retention of data that is inconsistent with the business context in which it is collected will frequently draw the ire of Commission regulators.[202] Third, companies have a continuing obligation to assess new threats and keep procedures and software up to date, and these obligations extend to vendors and temporary employees and contractors.[203]

Congress has called into question the FTC's reliance on vendor liability, with some critics arguing that the FTC uses vendors to inflate charges against the companies that are the primary targets of FTC.[204] Regardless, companies continue to be held liable for breaches caused by their vendors and contractors, whether through failure to adequately monitor them or failure to include contractual provisions mandating adequate security procedures.[205] However, even this would not serve to shield a company from liability if the FTC determined that the procedures being mandated by a company for its vendors were inadequate to begin with.[206]

Ultimately, while the FTC has issued recommendations for specific practices, such as securing remote access to servers and segmenting networks, it is unclear what combination of practices would be enough to avoid an enforcement action in the event a breach occurs despite the recommended protections.[207] With the growing number of high profile breaches of major retailers and financial providers, it is increasingly likely that the FTC will flex its newly affirmed authority even more in the coming months and years, which may shed more light on the specific practices that are truly seen as required for a reasonable data security program.

---

199 *See id.* at 1.

200 *See id.* at 2; *Prepared Statement of the Federal Trade Commission on Data Security*: *Hearing Before the H. Comm. on Energy & Commerce*, supra note 191, at 2–5.

201 *See* FED. TRADE COMM'N, START WITH SECURITY, *supra* note 150, at 2–3.

202 *See Prepared Statement of the Federal Trade Commission on Data Security*: *Hearing Before the H. Comm. on Energy & Commerce*, supra note 191, at 2–5.

203 *See* FED. TRADE COMM'N, START WITH SECURITY, *supra* note 150, at 10–12.

204 McGee, *supra* note 194.

205 *See, e.g., In re* GMR Transcription Servs, Inc., No. C-4502, 2014 WL 4252393, at *3–4 (F.T.C. Aug. 14, 2014); Complaint at 2–3, *In re* LabMD, Inc., No. 9357 (F.T.C. Aug. 28. 2013).

206 *See, e.g.*, *In re GMR Transcription Servs*, 2014 WL 4252393, at *3–4.

207 *See e.g.*, FTC v. Wyndham Worldwide Corp., 799 F.3d 236, 253–55 (3d Cir. 2015). *See generally* FED. TRADE COMM'N, START WITH SECURITY, *supra* note 150.

D. *Is Uncertainty Undermining Data Security?*

The Third Circuit's confirmation of the FTC's broad authority under Section 5 will give the Commission a more free hand in pursuing action against companies that are victimized by hackers.[208] However, by confirming the FTC's authority, the *Wyndham* decision has also removed any obligation for the FTC to provide more specific guidance on what it expects from a reasonable data security program. This section examines the potential uncertainty created by the *Wyndham* decision and the impact it may have on companies moving forward.

The major consequences of the current patchwork system of data security enforcement are high compliance costs and high uncertainty. The FTC currently performs only an abstract cost-benefit analysis under Section 5, which requires that the FTC balance the cost and availability of potential fixes with the potential harm to consumers of a violation.[209]

But this analysis does not require the FTC to specifically weigh the cost of its own enforcement actions against potential benefits to data security for consumers.[210] While the Commission does acknowledge factors such as cost of potential fixes and the sensitivity of the protected data in its enforcement analysis, it does not actually require proof of harm to individual consumers, and does not take adequate steps to tailor its consent decrees or its mandated data security practices to the scale of the company and the harm caused.[211]

This practice could have a chilling effect on innovation, as many smaller companies will not be able to afford the legal and compliance expertise necessary to stay on the right side of the FTC's reasonable and appropriate data security standard, and firms with the resources to comply may be hesitant to support innovative data security firms pioneering new technology or techniques in favor of using more established practices.[212] These firms may instead decide to rely on established techniques to avoid liability instead of sharing information and adopting innovative technologies that could help advance the field of cybersecurity to better respond to new threats. The Commission's newly confirmed broad authority could also make companies more hesitant to introduce new, experimental products that

---

208 *See*, *e.g.*, *Wyndham Worldwide Corp.*, 799 F.3d at 243, 257, 259.

209 *Id.* at 255–56; 15 U.S.C. § 45(n) (2012).

210 *Wyndham Worldwide Corp.* 799 F.3d at 255–56; 15 U.S.C. § 45(n).

211 The orders of consent decrees are substantially similar. *Compare, e.g.*, *In re GMR Transcription Servs*, 2014 WL 4252393, at *3–4, 6–9, *with In re* Accretive Health, Inc., No. C-4432, 2014 WL 726603, at *3–6 (F.T.C. Feb. 5, 2014).

212 Maureen K. Ohlhausen, Comm'r, FED. TRADE COMM'N, FTC-FCC: When is Two a Crowd, Address at the 33rd Annual Inst. on Telecomm. Policy & Regulation 5 (Dec. 4, 2015) ("If an enforcement action imposes costs disproportionate to the actual consumer harm, that enforcement action may make consumers worse off if prices rise or innovation slows.").

utilize sensitive data, including wearables, cloud-connected medical devices, and other big data-powered products associated with the "Internet of Things."[213]

All of these factors contribute to making a data breach more costly for companies in the U.S. than any other country.[214] As a result, more companies could choose to store or collect their data outside the United States, but this option has become more complicated with the recent European Court of Justice decision to invalidate the safe harbor program for companies transferring data from the EU to the U.S.[215]

Additionally, the increasing uncertainty over how data can be used and stored could lead to chilling effects on the technology sector, which is frequently dependent on unguided research using consumer data to improve and develop new products and offerings.[216] If the U.S. is to continue to lead the revolution in big data, companies must be assured that they have the freedom to collect and experiment with consumer data without incurring massive regulatory and civil liability. At the same time, a balance must be struck that ensures consumers are informed about how their data will be used when they sign up for a new service or consent to have their personal information collected, and consumers must have a clear avenue for redress in the event a company is truly negligent and becomes the victim of a hack. The best avenue to alleviate this uncertainty and safeguard consumers is for Congress to pass a comprehensive data security bill creating a uniform standard procedure to combat data breaches. The next section discusses some potential features of such a statutory regime.

---

213 *See* FED. TRADE COMM'N, INTERNET OF THINGS: PRIVACY & SECURITY IN A CONNECTED WORLD 1 (2015), https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf.

214 PONEMON INST., *supra* note 29, at 2; IBM, *supra* note 28, at app. 4.

215 Case C-362/14, Schrems v. Data Prot. Comm'r, 2015 E.C.R. I-35. As a result, "[a]bout 4,400 U.S. companies that are certified under the program must now quickly find other ways to lawfully transfer personal data outside the EEA." Stephen Gardner, *EU Data Transfer Path for U.S. Companies Invalidated*, BLOOMBERG BNA (Oct. 13, 2015). This decision comes at a time where cross-border data transfers and storage are becoming an increasingly large part of how companies handle data, with provisions to encourage such cross-border transfer and discourage data localization laws included in the Trans-Pacific Partnership Agreement recently signed by Australia, Brunei Darussalam, Canada, Chile, Japan, Malaysia, Mexico, New Zealand, Peru, Singapore, the U.S. and Vietnam. Trans-Pacific Partnership, ch. 14, 14-6 to -7, https://ustr.gov/trade-agreements/free-trade-agreements/trans-pacific-partnership/tpp-full-text; Donald G. Aplin, *Pacific Trade Pact Covers Data Transfer, Localization*, BLOOMBERG BNA (Nov. 9, 2015), http://www.bna.com/pacific-trade-pact-n57982063303/. *See also* Ronald W. Hovsepian, *Safe Harbor Invalidation Wake Up Call—All Industries Will Soon Be Regulated Industries: A Data Driven World Becomes a Privacy-Regulated Domain*, PRIVACY & SEC. L. REP. (Nov. 9, 2015).

216 *See* Ohlhausen, *supra* note 212, at 5, 7.

III. RECOMMENDATIONS

The uncertainty created by the FTC's broad authority to enforce data security standards has the potential to undermine data security by creating a chilling effect among companies, which may be reluctant to share information about new threats for fear of being held liable for negligent security practices.[217] This section examines possible solutions to clarify the standard of care for data security, and recommends that Congress provide clarity by enacting a statutory solution that shields non-negligent companies from liability and encourages information sharing that could lead to greater levels of protection for consumer data without the harmful effects of imposing massive liability on companies that are hacked.

With the ever increasing number and magnitude of data breaches reported in the U.S., it seems clear that the current patchwork system of data security standards is inadequate to handle the threat cyber attacks pose to the nation's economy and critical infrastructure. The current system creates a dangerous level of uncertainty that undermines innovation and creates massive compliance costs for businesses. As such, Congress should pursue statutory action to clarify the scope of the FTC's authority and the appropriate standard of care for data security practices, as well as bring uniformity to the current patchwork of state and federal enforcement regimes.

Empowering the FTC with broad, ambiguous powers to punish allegedly negligent businesses when hackers victimize them will not ensure that consumers are protected from breaches. Such a system will discourage the information sharing among businesses and security experts that is vital to address new hacking threats. With hacking tools becoming more sophisticated and widespread every day, federal regulators cannot be expected to keep pace without significant information sharing from businesses and cybersecurity experts. However, businesses will be reluctant to share information about new threats with the prospect of FTC unfairness liability hanging over their heads whenever a new vulnerability is discovered, especially when history demonstrates that it is a matter of "when," not "if" data will be exposed for most consumers. The solution does not lie in imposing massive liability on the companies that are victims of these hacks themselves, suffering massive reputational damage that can undermine revenue and stock performance for months and years.[218]

Instead, Congress should implement a system that returns the FTC to its original role as an enforcer of fair trade practices. As the *Wyndham* deci-

---

217 *See* Matt Flora, *Exclusive Q&A: Information Sharing From a Legal Perspective*, COMPASS CYBER SEC. BLOG (Aug. 26, 2015), http://www.compasscyber.com/blog/exclusive-qa-information-sharing-from-a-legal-perspective/; Brian Krebs, *Cybersecurity Information (Over)Sharing Act?*, KREBS ON SEC. (Oct. 27, 2015), http://krebsonsecurity.com/2015/10/cybersecurity-information-oversharing-act/.

218 *See* discussion of Target and other recent data breaches *supra* Section I.A.1.

sion shows, the courts are willing to enable an ever-broadening scope of power for the FTC as the nation's chief data security watchdog[219] – but the proper venue for setting the limits of the FTC's power is the legislature, not the courts. By passing a comprehensive data security statute, Congress can set clear boundaries on the FTC's authority, and codify areas in which the Commission can undertake enforcement actions. This will provide much-needed certainty to businesses and returning the FTC to its traditional focus of protecting consumers and promoting fair trade practices, not attempting to police technical practices in a rapidly changing industry, a task for which federal agencies are generally unsuited. While the FTC's current enforcement regime focuses on functional standards, its enforcement actions necessarily involve evaluating the technical details of a company's security program, a task that would be better accomplished by identifying relevant industry standards that both the Commission and private companies can look to when developing an evaluating a data security program.[220]

The current court and industry-specific statute based system is untenable, because it creates disparate outcomes based on industry and jurisdiction, resulting in a vacuum that the FTC and other regulatory agencies will rush to fill. Instead, Congress should empower the FTC to police misrepresentations of security policies and to lay out a framework that incorporates the process and function-based guidelines laid out in the PCI DSS and NIST standards, while limiting the ability of other agencies to pursue overlapping enforcement actions.

A sample framework that balances the relationship between Congress, the FTC, and the states can be found in COPPA. Like COPPA, Congress could enact a new overarching data security statute that gives the FTC authority to regulate data security using the Gramm-Leach-Bliley framework, which already forms the basis of much of the FTC's consent decrees. In such a statute, Congress could also implement COPPA-style safe harbors that limit liability for companies that comply with FTC-approved industry standards such as PCI-DSS or the NIST Cybersecurity Framework.

Congress should also pass targeted, industry-specific data breach notification statutes that would explicitly preempt state statutes and establish a uniform clearinghouse for data breach notifications. This would allow companies to fulfill notification requirements through a single process that then would filter out to the states and consumers, thereby eliminating the need to comply with a patchwork of state statutes. Such a statutory scheme would also give courts a uniform standard to apply in negligence actions, and should eliminate any private right to action, to ensure that the FTC is indeed the primary regulator of data security harms, instead of forcing the courts to attempt to create new tort and contract formulations based on the patchwork of federal, state, and industry standards and guidelines.

---

219 *See, e.g.*, FTC v. Wyndham Worldwide Corp., 799 F.3d 236, 248 (3d Cir. 2015).

220 *See* discussion of specific FTC enforcement actions *supra* Section II.C.

Using COPPA's framework in the data security context would minimize many of the concerns critics have raised around the law. COPPA has been criticized as "paternalistic" for placing additional obligations on parents to monitor what websites their children visit online, but a COPPA-like set of requirements for businesses would place no such additional requirements on individuals.[221] Additionally, while some have criticized COPPA for placing an overly onerous burden on small websites,[222] the current data security regime's patchwork of state and federal statutes already burdens companies in a far more onerous way with huge compliance costs and potential liability.[223] A uniform COPPA-like statute, rather than increase the regulatory burden on companies, would actually reduce the current compliance burden by standardizing notification obligations at the federal level and bringing clarity to the current uncertainty around FTC enforcement actions. Instead, a new federal data breach law could rely on COPPA-style safe harbors to reduce the FTC's role in penalizing companies while codifying the Commission's authority to regulate data security and encouraging the industry to police itself. This would spur innovation in the data security sector, as companies would be encouraged to develop new, more cost-effective security plans that meet the FTC's guidelines for approval. Thus, far from becoming a burden on companies, a new federal statute would be welcomed by the industry as a way to reduce compliance costs imposed by the current patchwork system.

CONCLUSION

We live in an age where if you are active online, the odds are good that your data will be exposed in a hack at some point, if it has not been already. The current data security regime prioritizes making companies who were victims themselves liable over encouraging the kind of clear standards and information sharing that could actually prevent more data breaches from occurring. In a world where nearly everyone may be the victim of a hack, there has to be a higher standard for liability than the fact that a breach occurred.

Currently, data security is governed by a patchwork system of federal law, agency regulations, and state statutes. This patchwork system has resulted in massive compliance costs for companies and has not reduced the number of consumers who have their data compromised by hackers every year. Additionally, the current system of FTC enforcement creates an environment where companies are unaware of what they must do to avoid liabil-

221 Allen, *supra* note 105, at 775–76.
222 Warmund, *supra* note 106, at 213–15.
223 *See supra* Section I.A.

ity, and are discouraged from sharing best practices and information about threats.

The recent Third Circuit decision in *Wyndham* only entrenches the problems in the current data security regime. By upholding the FTC's ability to pursue enforcement actions without giving clear guidance beforehand, the court increased the uncertainty that companies operate under, and the FTC's guidance is frequently inadequate to properly inform companies about what they must do to avoid liability. While the FTC can do a great deal of good by ensuring companies are operating with certain minimal protections for consumer data, its priorities must be increasing the overall level of data security and incentivizing innovation in this area, not imposing punitive sanctions on companies already facing the devastating consequences of a data breach.

Only through a uniform federal approach, spearheaded by Congress, can we develop a coherent policy of data security that will lead to more protection for everyone, both online and offline. Congress should take the lead on setting uniform standards that reduce the burden of complying with dozens of state and federal laws and restore the FTC to its proper consumer protection role. This will allow the Commission to focus on setting clear guidelines in conjunction with a robust safe harbor program that encourages industry self-regulation and incentivizes innovation in data security. With everyday transactions increasingly revolving around exchanges of consumer data, companies that store this information will only become greater targets for hackers, and Congressional inaction on this problem may only exacerbate the next big data breach, which is certainly coming.