CYBER INSECURITY: HOW *FTC v. WYNDHAM* FALLS SHORT AND WHY THE UNITED STATES STILL NEEDS FEDERAL LEGISLATION ADDRESSING MINIMUM CORPORATE CYBERSECURITY STANDARDS

STEPHANIE LOGAN DRUMM

INTRODUCTION 1
I. BACKGROUND 3
A. *A Brief History of Hacks* 4
B. *Federal Efforts to Address Corporate Cybersecurity Standards – The NIST Framework for Improving Critical Infrastructure Cybersecurity* 7
C. *The Evolution of the Federal Trade Commission's Cybersecurity Regulatory Authority and* Wyndham 8
II. WHY CORPORATE CYBERSECURITY STANDARDS NEED TO BE REGULATED 13
A. *The Current Regulatory Framework Has Been Unsuccessful and is Contrary to Public Policy* 13
1. Current Federal Cybersecurity Legislation Reflects a Narrow Approach, Which Overlooks Corporate Cybersecurity Standards 14
2. Corporations Need Concise Cybersecurity Regulation to Facilitate Corporate Compliance and Minimize Exposure to Liability. 16
3. The Commission's Attempts to Regulate Cybersecurity Practices Within its Current Statutory Authority have been Insufficient. 18
B. Wyndham *is Not a Permanent Solution to the Problem.* 20
III. CONGRESS SHOULD ENACT LEGISLATION DIRECTLY ADDRESSING CORPORATE CYBERSECURITY STANDARDS 24
A. *Option 1: Creating Statutory Corporate Cybersecurity Standards* 25
B. *Option 2: Expanding the FTCA to Encompass Cybersecurity Practices* 26
C. *Option 3: Enacting Legislation Delegating to the Commission Administrative Procedure Act Rulemaking Authority over Corporate Cybersecurity Practices* 28
CONCLUSION 33

INTRODUCTION

The security of consumer personal information has never been more at risk than it is today, and that risk is growing. An increasing number of large corporations are suffering data breaches, resulting in release of the personal and financial information belonging to millions of

consumers.[1] Every year, the occurrence of data breaches in the United States seems to get progressively worse.[2] In the United States, virtually all consumer transactions involve the use of personal information and credit cards.[3] Furthermore, the number of devices connected to the Internet of Things is rapidly increasing, with some experts predicting 90% of cars will be connected to the internet by 2020.[4] These trends arguably erase consumer choice to opt out and withhold personal information. As people become increasingly reliant on the security systems that companies employ to keep their personal and financial information private, and the Internet of Things[5] grows exponentially, there is now a critical need to uniformly regulate how this information is handled in order to protect consumers and national security. Almost every state has reacted in its own way with various data breach notification statutes.[6] However, there is currently no federal legislation regulating private corporate cybersecurity standards or delegating authority over these matters to a federal agency.[7]

The recent Third Circuit decision in *FTC v. Wyndham* appears on its face to be a solution to this problem, validating the Federal Trade Commission's ("Commission") authority over cybersecurity enforcement by interpreting "unfair competition" to include deficient cybersecurity

---

[1] *See infra* Part I.A.
[2] *See* DJ Pangburn, *2013 Was the Worst Year for Data Breaches*, MOTHERBOARD (Jan. 23, 2014), http://motherboard.vice.com/blog/2013-was-the-worst-year-for-data-breaches; Petr Svab, *2014 Worst Year Ever for Data Breaches*, EPOCH TIMES (Feb. 27, 2015), http://www.theepochtimes.com/n3/1266470-2014-worst-year-ever-for-data-breaches-added-5-worst-cyberhacks-to-top-10/; Illena Armstrong, *Will 2011 Be Coined Year of the Breach?*, Perspectives Newsletter Iss. 4 EXPERIAN, Winter 2012, http://www.experian.com/data-breach/newsletters/2011-year-of-the-breach.html.
[3] *See* Brief for the Federal Trade Commission at 2, F.T.C. v. WYNDHAM HOTELS & RESORTS, LLC, No. 13-01887, 2014 WL 6629142 (stating "[v]irtually all modern commerce involves the collection and storage of consumers' personal data, such as credit card numbers, passwords, and social security numbers").
[4] *Connected Car Industry Report 2013*, TELEFONICA 9 (2013), http://websrvc.net/2013/telefonica/Telefonica%20Digital_Connected_Car2013_Full_Report_English.pdf.
[5] Oxford dictionary defines the Internet of Things as "The interconnection via the Internet of computing devices embedded in everyday objects, enabling them to send and receive data." OXFORD DICTIONARIES, http://www.oxforddictionaries.com/definition/english/internet-of-things.
[6] *See infra* Part II.A.2.
[7] *See infra* Part II.A.1.

practices.[8] However, this is only a temporary solution to a larger problem. The *Wyndham* decision merely allows the Commission to step in *after* a company has already violated the FTCA. Such enforcement power does nothing to pre-emptively protect the American public's personal information from initial exposure. Federal legislation is still needed to delegate prophylactic rulemaking authority to the Commission, allowing the United States to take steps to prevent data breaches before they happen.[9] This Comment argues that, to prevent the occurrence of future data breaches, Congress should delegate to the Commission Administrative Procedure Act ("APA") rulemaking authority to promulgate and enforce mandatory information security standards for all companies using, storing, and transmitting consumer personal and financial information, including information transmitted via products within the Internet of Things.

Part I explores the background of data breaches and cybersecurity regulation in the United States and concludes with a discussion of the recent Third Circuit decision in *Wyndham* and its impact on the Commission's authority over cybersecurity regulation. Part II will examine the shortcomings in the current cybersecurity regulatory framework. Part II will then delve into why prophylactic cybersecurity legislation is needed and would better serve the public than remedial measures such as enhanced consumer remedies or increased liability for companies that expose consumer information. Finally, Part III will discuss the possible legislative approaches to regulating this area and argue that the best approach is enacting legislation delegating to the Federal Trade Commission APA rulemaking authority over corporate cybersecurity practices.

I. BACKGROUND

The insufficiency of corporate data security practices has become a serious problem, which is rapidly growing. Both large and small businesses alike are suffering from data breaches,

[8] *See infra* Part I.B.
[9] *See infra* Part II.

resulting in massive losses of both corporate and consumer dollars. The federal government has failed to address the critical need to regulate this area, and has left the Commission to do its best to fill in the gaps in legislation in the absence of explicit authority. Section A will discuss the multi-billion dollar corporate exposure to liability resulting from insufficient data security practices by examining recent high-profile hacks of large companies. Section A will then discuss how this risk is not limited to large companies, but can be just as detrimental for smaller companies. Section B describes the current (inadequate) regulatory framework and federal attempts to address corporate cybersecurity standards. Section C will examine the evolution of the Commission's rise to the top of cybersecurity regulation in the United States, ending with the recent Third Circuit decision in *Wyndham*.

A. A Brief History of Hacks

Over the past five years, companies in the United States have lost of billions of dollars due to data breaches resulting from insufficient cybersecurity practices.[10] One of the largest and earliest data breaches involving consumer information targeted TJX, the parent company of retail stores such as T.J. Maxx and Marshalls. This breach alone impacted at least 94 million customers.[11] Insufficient data security practices caused the data breach,[12] which resulted in at

[10] *See 11 data breaches that stung U.S. Customers*, BANKRATE (last visited Nov. 15, 2015), http://www.bankrate.com/finance/banking/us-data-breaches-3.aspx.
[11] Julianna Pepitone, *5 of the biggest-ever credit card hacks*, CNNMONEY (Jan.12, 2014), http://money.cnn.com/gallery/technology/security/2013/12/19/biggest-credit-card-hacks/3.html.
[12] Specifically, the Commission charged that TJX's insufficient data security practices included (1) storing and transmitting consumer payment information in clear text, (2) failing to use readily available security measures to limit wireless access to its networks, (3) failing to implement required password strengthening policies, (4) failing to use readily available security measures, including firewalls, and (5) failing to employ sufficient measures to detect and prevent unauthorized access to its networks. Press Release, Fed. Trade Comm'n, Agency Announces Settlement of Separate Actions Against Retailer TJX, and Data Brokers Reed Elsevier and Seisint for Failing to Provide Adequate Security for Consumers Data (Mar. 27, 2008), https://www.ftc.gov/news-events/press-releases/2008/03/agency-announces-settlement-separate-actions-against-retailer-tjx.

least $118 million worth of liability for TJX,[13] and a Commission settlement requiring twenty years of monitoring.[14]

Other massive data breaches include the breach of Target, Inc.'s point-of-sale systems in late 2013, which exposed the personal and financial information of up to 70 million individuals, and resulted in $290 million in company data breach-related expenses.[15] A similar data breach at Home Depot exposed the personal and financial information of up to 57 million individuals and cost the company $252 million as of November 1, 2015.[16] In one of the most interesting recent hacks, Ashley Madison, a dating website for married people, was notoriously hacked in June 2015, resulting in public exposure of the identities of its more than 32 million users.[17] In addition to the standard privacy issues at stake, this hack represented something greater– reputational loss to consumers that had a profound impact on lives, possibly even contributing to two suicides.[18]

Another major incident occurred between 2008 and 2009 when Wyndham Worldwide Hotels suffered three separate data breaches due to deficient data security practices, which

---

[13] *TJX, Visa reach $40.9M Settlement for data breach*, USATODAY (Nov. 30, 2007), http://usatoday30.usatoday.com/money/industries/retail/2007-11-30-tjx-visa-breach-settlement_N.htm.
[14] Press Release, Fed. Trade Comm'n, Agency Announces Settlement of Separate Actions Against Retailer TJX, and Data Brokers Reed Elsevier and Seisint for Failing to Provide Adequate Security for Consumers Data (Mar. 27, 2008), https://www.ftc.gov/news-events/press-releases/2008/03/agency-announces-settlement-separate-actions-against-retailer-tjx.
[15] Target Corp. Quarterly Report Pursuant to Section 13or 15(d) of the Securities Exchange Act of 1934 For the quarterly period ended October 31, 2015 10-11 (Nov. 25, 2015), http://www.sec.gov/Archives/edgar/data/27419/000002741915000029/tgt-20150801x10xq.htm.
[16] Home Depot Quarterly Report Pursuant to Section 13or 15(d) of the Securities Exchange Act of 1934 For the quarterly period ended November 1, 2015, 16-17 (Nov. 24, 2015), http://www.sec.gov/Archives/edgar/data/354950/000035495015000033/hd_10qx08022015.htm.
[17] Robert Hackett, *What to Know About the Ashley Madison Hack*, FORTUNE (Aug. 26, 2015), http://fortune.com/2015/08/26/ashley-madison-hack/.
[18] *See* Laurie Segall, *Pastor outed on Ashley Madison commits suicide*, CNNMONEY (Sep. 8, 2015), http://money.cnn.com/2015/09/08/technology/ashley-madison-suicide/; Albert Salazar, *City Employee With Email Address Linked to Ashley Madison Committed Suicide*, SAN ANTONIO CURRENT (Aug. 21, 2015), http://www.sacurrent.com/Blogs/archives/2015/08/21/city-employee-with-email-address-linked-to-ashley-madison-committed-suicide.

exposed over 600,000 records and caused consumers to lose almost $11 million.[19] Wyndham's expenses are still mounting as it continues to defend itself in litigation with the Commission.[20]

Although these high-profile attacks draw the most attention, numerous hacks of smaller companies also occur, often going unnoticed.[21] As the founder and chief executive of Billguard, Yaron Samid, phrased it, "[w]hen you have a national brand, then it becomes major news . . . A lot of smaller merchants get breached all the time."[22] In fact, according to the House Small Business Committee, "71% of cyber-attacks occur at businesses with fewer than 100 employees."[23] This should not come as a surprise, considering 83% of small businesses have no formal cybersecurity plan in place, and 69% have no plan in place at all.[24] The economic impact of these data breaches is even more disturbing, with almost two-thirds of small companies that fall victim to a data breach going out of business within six months.[25] Data breaches impact almost every company—in 2009 alone, data breaches may have impacted 85% of U.S. companies at least once, leading to billions of dollars in expenses for American businesses.[26] Companies expend extensive resources in an effort to combat this problem, spending an estimated $75 billion annually on cybersecurity as of 2015.[27] This issue impacts companies both

[19] *See infra* Part I.C.2.
[20] *Id.*
[21] *See* H. SMALL BUS.COMM., SMALL BUSINESS, BIG THREAT: PROTECTING SMALL BUSINESSES FROM CYBER ATTACKS, (Apr. 22, 2015), http://smallbusiness.house.gov/news/documentsingle.aspx?DocumentID=398099.
[22] *11 data breaches that stung U.S. Customers*, *supra* note 10.
[23] *Id.*
[24] John Patrick Pullen, *How to Protect your Small Business Against a Cyber Attack*, ENTREPRENEUR (Feb. 27, 2013), http://www.entrepreneur.com/article/225468.
[25] *Id.*
[26] *The Liability of Technology Companies for Data Breaches*, ADVISEN 1 (2010), https://www.advisen.com/downloads/Emerging_Cyber_Tech.pdf.
[27] Gil Press, *This Week In Tech History: The Birth Of The Cybersecurity And Computer Industries*, FORBES (Nov. 1, 2015, 12:03 PM), http://www.forbes.com/sites/gilpress/2015/11/01/this-week-in-tech-history-the-birth-of-the-cybersecurity-and-computer-industries/.

large and small in a severe way, and these companies need guidance and incentive to protect themselves and consumers from the detrimental effects of data breaches.

B. Federal Efforts to Address Corporate Cybersecurity Standards – The NIST Framework for Improving Critical Infrastructure Cybersecurity

Despite the Federal government's recent increasing focus on cybersecurity, it has made minimal efforts to address corporate cybersecurity standards.[28] The federal government's primary achievement in this area is the United States Department of Commerce's National Institute of Standards and Technology (NIST) Framework for Improving Critical Infrastructure Cybersecurity.

In 2014, in response to Executive Order 13636, the NIST published the NIST Framework for Improving Critical Infrastructure Cybersecurity.[29] This framework outlined voluntary measures that organizations should take in order to reduce cybersecurity risks.[30] President Obama prompted all federal agencies to analyze their own cybersecurity practices against this framework, and these practices have also caught on in the private sector.[31] Congress' approval of the NIST's efforts came in the form of The Cybersecurity Enhancement Act of 2014, which authorized the NIST to develop a "voluntary, consensus-based, industry-led set of standards and procedures to cost-effectively reduce cyber risks to critical infrastructure."[32] On a simplified level, such practices encourage developing and implementing policies and procedures to address and continuously monitor five primary functions of cybersecurity systems: (1) identify the needs

[28] *See President Obama Signs Five Cybersecurity-related Bills*, Practical Law Legal Update 6-593-6567 (Dec. 23, 2014).
[29] Richard Raysman and John Rogers, *The NIST Cybersecurity Framework*, Practical Law Practice Note 5-599-6825.
[30] *Id.*
[31] *Id.*
[32] Congress, S.1353 – Cybersecurity Enhancement Act of 2014 Action Overview (last visited Nov. 15, 2015), https://www.congress.gov/bill/113th-congress/senate-bill/1353.

of a specific organization; (2) protect systems against a cybersecurity event; (3) detect the occurrence of a cybersecurity event; (4) respond to a cybersecurity event; and (5) recover from a cybersecurity event.[33]

Although these comprehensive best practices are voluntary, a growing number of private organizations are looking to them as a "de facto framework" for developing and implementing data security plans.[34] Despite this trend and the availability of this helpful resource, companies large and small are still failing to implement data security plans.[35]

C. The Evolution of the Federal Trade Commission's Cybersecurity Regulatory Authority and Wyndham

In the absence of federal legislation, the Commission has worked since 2002 to use its authority under the FTCA to partially fill in the cavernous gap in the area of corporate cybersecurity practices.[36] Its uphill battle over the last fourteen years culminated in 2015 with *Wyndham*, which industry experts hoped would solve the problem that Congress has failed to address.[37]

The Commission derives its consumer protection authority from the Federal Trade Commission Act of 1914 ("FTCA") which, as amended, deems unlawful any "unfair methods of competition . . . and unfair or deceptive acts or practices in or affecting commerce."[38] Legislative history shows that Congress intentionally omitted any specific definition of "unfair"

---

[33] NIST Cybersecurity Framework, *supra* note 29.
[34] NIST Cybersecurity Framework, *supra* note 29.
[35] *See supra* Part I.A.
[36] *See* Fed. Trade Comm'n, U.S. Federal Trade Commissioner Julie Brill Keynote Address Before the Center for Strategic and International Studies 3 (Sep. 17, 2014), https://www.ftc.gov/system/files/documents/public_statements/582841/140917csisspeech.pdf.
[37] *See* Third Circuit Hears Oral Arguments in FTC v. Wyndham, HUNTON & WILLIAMS PRIVACY & INFORMATION SECURITY LAW BLOG (Mar. 5, 2015) https://www.huntonprivacyblog.com/2015/03/05/third-circuit-hears-oral-arguments-ftc-v-wyndham/.
[38] 15 U.S.C.A. § 45(a)(1) (West 2012).

in order to allow the Commission the flexibility to adapt the statute to apply to a wide variety of existing and evolving areas.[39] The Commission's application of the FTCA to the area of data security began in 2002 with an initial focus on the deception prong of Section 5 of the FTCA.[40] The agency quickly realized that it could also use its power to regulate unfair business practices under the FTCA to further protect consumers and their personal information from insufficient data security practices and brought its first pure "unfairness" action in 2005.[41] Since then, the Commission has brought over fifty enforcement actions against various U.S. companies for failure to maintain reasonable data security practices[42] and has emerged as the leading federal agency in policing corporate data security practices.[43]

Although some critics claim that the Commission's efforts to regulate cybersecurity have resulted in unclear standards and fail to provide guidance to businesses,[44] strong evidence points to the contrary.[45] As part of its mission to protect consumers and promote data security practices by educating consumers and businesses, the Commission has committed substantial resources to providing a wealth of guidance and information concerning data-security practices to businesses, including its business guide to data security, basic security issues for businesses, educational

---

[39] *F.T.C. v. Wyndham Worldwide Corp*, 799 F.3d 236, 243 (2015) (hereinafter *Wyndham*).
[40] Fed. Trade Comm'n, U.S. Federal Trade Commissioner Julie Brill Keynote Address Before the Center for Strategic and International Studies 3 (Sep. 17, 2014), https://www.ftc.gov/system/files/documents/public_statements/582841/140917csisspeech.pdf.
[41] *Id*.at 4.
[42] Fed. Trade Comm'n, Privacy & Security Update (2014) (Jan. 2015), https://www.ftc.gov/reports/privacy-data-security-update-2014.
[43] *See* Katy Bachman, FTC Chair Edith Ramirez Fights for Data Security and Privacy Rights Consumers, ADWEEK (May 27, 2014), http://www.adweek.com/news/television/ftc-chair-edith-ramirez-fights-data-security-and-privacy-rights-157930.
[44] *See* Michael D. Simpson, *All Your Data Are Belong to Us: Consumer Data Breach Rights and Remedies in an Electronic Exchange Economy*, Univ. of Colo. L. Rev. at [29] (2016). [Cite to be completed when published]
[45] *See* Fed. Trade Comm'n, FTC Prepared Statement 5-6 (June 15, 2011), https://www.ftc.gov/sites/default/files/documents/public_statements/prepared-statement-federal-trade-commission-data-security/110615datasecurityhouse.pdf; Data Security, Federal Trade Commission, (last visited Nov. 15, 2015), https://www.ftc.gov/tips-advice/business-center/privacy-and-security/data-security.

tools, workshops, and comprehensive guidelines on best practices.[46] The Commission has devoted an entire section of its website to data security materials for businesses, which includes guidance materials, videos, a business blog, and links to legal resources on data security.[47] In 2015, the Commission launched its "Start with Security" business education initiative, which provides thorough educational resources for businesses, and holds events in cities around the country to educate businesses in implementing effective data security programs.[48]

In August 2015, the Commission's fight to assert authority over cybersecurity regulation gained its first appellate stamp of approval by the Third Circuit in *Federal Trade Commission v. Wyndham Worldwide Corporation, et al.*, when the court upheld the district court's rejection of Wyndham's motion to dismiss the case for failure to state a claim.[49] Between 2008 and 2009, Wyndham, the world's largest hotel company,[50] suffered three separate major data breaches that exposed the personal information of over half a million consumers and resulted in over $10.6 million in fraudulent charges.[51] The Commission filed suit against Wyndham in 2012, alleging that Wyndham engaged in both "unfair" and "deceptive" practices by "failing to employ reasonable and appropriate measures to protect personal information against unauthorized access" and misrepresenting in their privacy policy that they had implemented those protective

[46] Fed. Trade Comm'n, FTC Prepared Statement 5-6 (June 15, 2011), https://www.ftc.gov/sites/default/files/documents/public_statements/prepared-statement-federal-trade-commission-data-security/110615datasecurityhouse.pdf.
[47] *See* Data Security, Federal Trade Commission, (last visited Nov. 15, 2015), https://www.ftc.gov/tips-advice/business-center/privacy-and-security/data-security.
[48] Press Release, Fed. Trade Comm'n, *FTC Kicks Off "Start With Security" Business Education Initiative* (June 30, 2015), https://www.ftc.gov/news-events/press-releases/2015/06/ftc-kicks-start-security-business-education-initiative; *see also* Fed. Trade Comm'n, Start with Security: A Guide for Business (last visited Nov. 15, 2015), https://www.ftc.gov/tips-advice/business-center/guidance/start-security-guide-business.
[49] *F.T.C. v. Wyndham Worldwide Corp*, 799 F.3d 236 (2015).
[50] *Our Company*, Wyndham Worldwide (last visited Nov. 14, 2015), http://www.wyndhamworldwide.com/category/wyndham-hotel-group.
[51] *Wyndham* at 240.

measures.[52] Specifically, the Commission alleged that Wyndham engaged in unfair business practices by storing payment information in clear readable text; allowing its employees and franchisees to use easily-guessed passwords to access its property management system; failing to utilize firewalls; failing to restrict third-party access to its network and hotel servers; and failing to use reasonable measures to detect, prevent, investigate, and respond to unauthorized access to its network.[53]

Wyndham moved to dismiss both claims, asserting, among other things, that the Commission's unfairness authority does not extend to data security, and the Commission failed to give fair notice of what data security practices are required under Section 5 of the FTCA.[54] The District court denied the motion to dismiss, and the Third Circuit Court of Appeals granted interlocutory appeal as to two issues related to the unfairness claim: (1) "whether the Commission has authority to regulate cybersecurity under the unfairness prong", and (2) "if so, whether Wyndham had fair notice its specific cybersecurity practices could fall short of that provision."[55]

After a thorough analysis of the historical, judicial, and legislative development of the Commission's enforcement authority in areas of consumer protection, and the plain meaning of the word "unfair," the court rejected Wyndham's arguments challenging the Commission's unfairness authority over data security practices. The court found that the meaning of "unfair" in Section 5 of the FTCA includes insufficient cybersecurity practices resulting in substantial harm

[52] FTC Complaint, F.T.C. v. Wyndham Worldwide, No. 13-01887 (2012), 2012 WL 12146600 (D.N.J.).
[53] *Wyndham* at 240-41.
[54] Motion to Dismiss by Defendant Wyndham Hotels & Resorts LLC, FTC v. Wyndham Worldwide Corp., No. 13-01887 (2012), 2012 WL 12146600 (D.N.J.).
[55] *Wyndham* at 240.

to consumers.[56] Additionally, the court analyzed and rejected Wyndham's fair notice objection, citing the surrounding circumstances as strong evidence in favor of the Commission.[57] Such evidence included Wyndham's complete lack of critical cybersecurity systems, that it had been hacked three times, that the Commission issued a guidebook on sound cybersecurity practices for businesses, and that the Commission had brought several prior administrative cases interpreting inadequate corporate cybersecurity to fall under the umbrella of unfair practices.[58]

The decision marked the first time that a federal appellate court validated the Commission's enforcement authority over inadequate data security practices.[59] It validated the Commission's data security efforts since 2002 and solidified the Commission's pivotal role in data security enforcement going forward.[60] Under this structure, the Commission uses a reasonableness standard for evaluating a company's cybersecurity practices.[61] The Commission describes reasonableness as:

> …reasonable and appropriate in light of the sensitivity and volume of consumer information it holds, the size and complexity of its business, and the cost of available tools to improve security and reduce vulnerabilities. Through its settlements, testimony, and public statements, the Commission has made clear that it does not require perfect security; reasonable and appropriate security is a continuous process of assessing and addressing risks.[62]

Some experts have lauded this decision as a solution to the problem, while the Commission has characterized it as merely "reaffirming" the Commission's authority over data

---

[56] *Id.* at 243.
[57] *Id.* at 256.
[58] *Id.* at 255-59.
[59] Richard Martinez, *Third Circuit rules in FTC v. Wyndham case -- The decision is a must-read for business executives and attorneys*, LinkedIn, (Aug. 25, 2015), https://www.linkedin.com/pulse/third-circuit-rules-ftc-v-wyndham-case-decision-richard-martinez.
[60] Third Circuit rules in FTC v. Wyndham case, FTC BUSINESS BLOG (AUG. 25, 2015), https://www.ftc.gov/news-events/blogs/business-blog/2015/08/third-circuit-rules-ftc-v-wyndham-case.
[61] Fed. Trade Comm'n, Commission Statement Marking the FTC's 50th Data Security Settlement 1 (Jan 31, 2014), https://www.ftc.gov/system/files/documents/cases/140131gmrstatement.pdf.
[62] *Id.* at 1.

security.[63] However, as Part II.B argues, *Wyndham* is not a sufficient solution to the major data security regulatory problem in the United States.

II. WHY CORPORATE CYBERSECURITY STANDARDS NEED TO BE REGULATED

The current regulatory framework surrounding corporate cybersecurity practices is a haphazard mishmash of state and federal laws that are constantly changing. These existing laws fail to protect consumers because they merely punish companies after a breach has happened and do not incentivize or require companies to proactively protect against data breaches. In order to effectively protect consumers against loss of personal information, and even personal safety with the growing Internet of Things, Congress needs to pass prophylactic cybersecurity legislation.

Section A explores the deficiencies in the current regulatory framework surrounding corporate cybersecurity practices, including a lack of Federal legislation directly addressing the problem; the corporate need for a workable, uniform regulatory framework; and the insufficiency of the Commission's attempts to regulate within its current regulatory authority. Section A concludes with further policy justifications in favor of prophylactic Federal cybersecurity legislation, such as expert predictions of a "major cyberattack," the preventability of most data breaches, and the growing concern regarding the critically unsecure Internet of Things. Part B explores why the court's decision in *Wyndham* is not an adequate substitute for federal legislation.

A. The Current Regulatory Framework Has Been Unsuccessful and is Contrary to Public Policy

[63] Fed. Trade Comm'n, Statement from FTC Chairwoman Edith Ramirez on Appellate Ruling in the Wyndham Hotels and Resorts Matter (Aug 24, 2015), https://www.ftc.gov/news-events/press-releases/2015/08/statement-ftc-chairwoman-edith-ramirez-appellate-ruling-wyndham.

According to the Pew Research Center, 61% of experts believe that a "major cyberattack" will have "caused widespread harm to a nation's security and capacity to defend itself and its people" by the year 2025.[64] One expert emphasized the importance of implementing adequate measures to protect critical infrastructure because the speed at which the "level of sophistication of adversaries generally progresses [is] much faster."[65] While some experts are confident that countermeasures will improve in that timeframe, others expressed concern that there is a lack of political incentive and motivation to address even the most minimal cybersecurity standards.[66] Some officials in the Obama administration have gone so far as to warn of an impending "Cyber Pearl Harbor."[67] This massive potential risk underlies the need for some sort of regulation in this area. However, as this Section will explain, there have been no real attempts by Congress to address this issue, and the Commission's attempts to do something within its current statutory authority are not an adequate substitute.

Subsection 1 will discuss the lack of federal legislation addressing the issue of minimum corporate cybersecurity standards in the United States. Subsection 2 will discuss the evidence that such regulation is, in fact, needed by corporations struggling to comply with the current piecemeal cybersecurity regulatory framework in the United States. Subsection 3 will then explore how the Commission's attempts to regulate cybersecurity within its current legislative authority have been insufficient.

1. Current Federal Cybersecurity Legislation Reflects a Narrow Approach, Which Overlooks Corporate Cybersecurity Standards

[64] Lee Rainie, Janna Anderson and Jennifer Connolly, *Cyber Attacks Likely to Increase*, PEW RESEARCH CENTER (Oct. 29, 2014), http://www.pewinternet.org/2014/10/29/cyber-attacks-likely-to-increase/
[65] *Id.*
[66] *Id.*
[67] *Id.*

While the federal government has made significant progress over the past few years in passing cybersecurity legislation and regulations, it has focused the bulk of its efforts on national security, leaving a void where corporations are concerned. In fact, almost all of the federal government's increased efforts to protect consumer information have focused on reactive, rather than proactive measures.[68] Only recently has the government even started looking toward updating its own systems to meet some sort of cybersecurity standards,[69] but it only did so as a reaction to the detrimental hack of the Office of Personnel Management in June 2015.[70] This constricted approach to the battle against cybercrime is incomplete and ignores other approaches that can and should be employed to prevent data breaches before they happen. The federal government needs a multifaceted approach to battling cybercrime in order to efficiently protect the nation's cybersecurity defenses and economy. Recent government actions, including legislation and executive orders, have addressed information sharing, criminal consequences, and increased federal cybersecurity measures, but have yet to implement any measures attacking the problem from the corporate side.[71]

Moreover, from a consumer protection perspective, mere remedial punitive liability for corporate failure to implement adequate security measures is insufficient because it does not

---

[68] *See* David Hudson, *The President Announces New Actions to Protect Americans' Privacy and Identity*, THE WHITE HOUSE (Jan. 12, 2015), https://www.whitehouse.gov/blog/2015/01/12/president-announces-new-actions-protect-americans-privacy-and-identity.

[69]The Cybersecurity Strategy Implementation Plan was announced on October 30, 2015, which follows a 30-day Cybersecurity Sprint carried out by the Federal government in an attempt to update all of its legacy systems. Tony Scott, *Modernizing Federal Cybersecurity*, THE WHITE HOUSE (Oct. 30, 2015, 3:00 PM), https://www.whitehouse.gov/blog/2015/10/30/modernizing-federal-cybersecurity.

[70] Devin Coldewey, *White House Details Plan to Bring Cybersecurity Up to Date*, NBC NEWS (Oct. 30, 2015, 7:42 PM), http://www.nbcnews.com/tech/security/white-house-details-plan-bring-feds-cybersecurity-date-n454861. The hack resulted in the exposure of personal information, including social security numbers and fingerprints, of 21.5 million people. Press Release, Office of Personnel Management, OPM Announces Steps to Protect Federal Workers and Others From Cyber Threats (July 9, 2015), https://www.opm.gov/news/releases/2015/07/opm-announces-steps-to-protect-federal-workers-and-others-from-cyber-threats/.

[71] *See* FACT SHEET: Administration Cybersecurity Efforts, THE WHITE HOUSE (July 9, 2015), https://www.whitehouse.gov/the-press-office/2015/07/09/fact-sheet-administration-cybersecurity-efforts-2015.

make the implementation of data security plans mandatory. This risk of possible future liability is not enough to incentivize corporations to expend time and resources on developing and executing a plan. Indeed, many corporations have already established that, in the absence of mandatory regulations, they will choose to risk consumer information and not implement such data security plans.[72] While remedial damages can help consumers in the event of a data breach, their personal information can never be re-secured. And in situations such as the Ashley Madison hack, involving serious reputational loss to consumers, those consumers could never be made whole again through monetary damages.

While remedial legislation such as increasing consumer legal remedies in the event of a data breach may serve to help make consumers whole again, it does nothing to proactively protect consumers. In order to adequately protect consumers and businesses, in addition to remedial punitive measures, legislation should also provide proactive measures to protect consumer personal information from being exposed in the first place.

2. Corporations Need Concise Cybersecurity Regulation to Facilitate Corporate Compliance and Minimize Exposure to Liability.

As it stands, the current regulatory framework forces companies to piece together several fragments of state and federal legislation in order to develop fully-compliant cybersecurity policies. As of 2013, there were over fifty active federal statutes directly or indirectly addressing cybersecurity issues, and yet no overarching framework legislation exists.[73] Furthermore, numerous administrative agency activities touch on corporate cybersecurity practices in one way or another, including the Department of Homeland Security, the Securities and Exchange

[72] *See infra* Part II.A.3.
[73] ERIC A. FISCHER, CONG. RESEARCH SERV., R42114, FEDERAL LAWS RELATING TO CYBERSECURITY OVERVIEW AND DISCUSSION OF PROPOSED REVISIONS 2 (June 20, 2013), http://fas.org/sgp/crs/natsec/R42114.pdf.

Commission, the Federal Trade Commission, and the Secretary of Health and Human Services.[74] In addition to federal legislation and administrative regulation, forty-seven states, the District of Columbia, Guam, Puerto Rico and the Virgin Islands have each developed their own information security regulations, creating fifty-one different interpretations of notice requirements, what constitutes a breach, who is covered, exemptions from legislation, and definitions of "personal information."[75] Not only do these definitions differ in significant ways, but in some instances they are contradictory.[76]

Moreover, these laws are constantly changing—at least thirty two states were considering new or amended legislation in 2015.[77] Three states have gone so far as to pass laws making businesses liable to financial institutions for payment of card information breach-related costs.[78] For companies operating nationwide, this regulatory framework creates an extremely complicated landscape to navigate. A number of cases have also invoked state tort liability.[79] Inadequate cybersecurity practices can also result in company shareholder derivative action and potential individual liability for board members.[80] After Target's massive data breach in 2013,

---

[74] *Id.* at 52-61 tbl. 2.
[75] Security Breach Notification Laws, Nat'l Conference of State Legislatures (Oct. 22, 2015), http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx.
[76] *See* Rachael M. Peters, *So You've Been Notified, Now What? The Problem with Current Data-Breach Notification Laws*, 56 ARIZ. L. REV. 1171, 1183 (2014) (discussing that while the notice-of-breach laws in some states require notice of breach to be delivered to consumer within a specified number of days, other states do not allow notice to be delivered until analysis of the breach's risk-of-harm has been completed).
[77] 2015 Security Breach Legislation, Nat'l Conference of State Legislatures (June 11, 2015), http://www.ncsl.org/research/telecommunications-and-information-technology/2015-security-breach-legislation.aspx.
[78] The Liability of Technology Companies for Data Breaches, ADVISEN 3 (2010), https://www.advisen.com/downloads/Emerging_Cyber_Tech.pdf.
[79] Stewart Baker, The Volokh Conspiracy, *Why tort liability for data breaches won't improve cybersecurity*, WASHINGTON POST (Jan. 11, 2015), https://www.washingtonpost.com/news/volokh-conspiracy/wp/2015/01/11/why-tort-liability-for-data-breaches-wont-improve-cybersecurity/
[80] *See* Kevin M. LaCroix, *Wyndham Worldwide Board Hit with Cyber Breach-Related Derivative Lawsuit*, LEXISNEXIS (May 7, 2014), http://www.lexisnexis.com/legalnewsroom/corporate/b/blog/archive/2014/05/07/wyndham-worldwide-board-hit-with-cyber-breach-related-derivative-lawsuit.aspx; In such shareholder derivative action, standard Director and

the company found itself involved in almost all of these varieties of litigation, including (1) two shareholder derivative actions against the company's directors and officers;[81] (2) litigation brought by all four major payment card networks; (3) over 100 actions brought in various states by customers, shareholders, and banks; and (4) investigations by multiple State Attorneys General, the Federal Trade Commission, and the Securities and Exchange Commission, many of which are still ongoing over two years later.[82]

In light of this massive potential for liability, it comes as no surprise that cybersecurity is one area where CEOs actually want more regulation and guidance in order to know how to adequately protect their companies.[83] Federal regulation of cybersecurity standards would undoubtedly benefit companies as well as consumers. A clear set of standards would enable companies to easily comply with regulations, minimize exposure to liabilities, and better protect themselves from intruders.

3. The Commission's Attempts to Regulate Cybersecurity Practices Within its Current Statutory Authority have been Insufficient.

The Commission has made many data security resources available to the public for almost fifteen years, and yet companies choose to continue putting consumer data at risk by not implementing these voluntary measures.[84] The multitude of high-profile hacks and astounding statistics related to small-business data security practices are strong evidence that U.S. businesses

---

Officer insurance might not indemnify the company directors and officers in the event of a settlement or court award, leaving them responsible for paying everything out of pocket. Ann Longmore, *Directors Sued for Cyber Breach*, WILLISWIRE (Feb. 20, 2014), http://blog.willis.com/2014/02/directors-sued-for-cyber-breach/

[81] Kevin LaCroix, *Target Directors and Officers Hit with Derivative Suits Based on Data Breach*, THE D&O DIARY (Feb. 3, 2014), http://www.dandodiary.com/2014/02/articles/cyber-liability/target-directors-and-officers-hit-with-derivative-suits-based-on-data-breach/

[82] Target Corp., *supra* note 15.

[83] *See* Melissa Maleske, *Why Every Company Needs a Cyberbreach Plan*, LAW360 (Oct 21, 2015, 7:34 PM), http://www.law360.com/articles/716931/why-every-company-needs-a-cyberbreach-plan.

[84] *See* FTC Prepared Statement, *supra* note 46.

are ignoring the government's guidance and best practices regarding cybersecurity practices.[85] The "voluntary measures" approach appears to have failed.

Despite the availability of thorough resources promulgated by the Commission, and development of voluntary best practices by the NIST, companies are still choosing not to implement data security systems. As previously examined, almost 70% of small businesses have no data security plan in place.[86] According to Verizon's 2012 Data Breach Investigation Report, 97% of breaches in 2011 were avoidable "through simple or intermediate controls."[87] Experience has proven that the current structure of voluntary recommendations is not working, and something needs to change.

This rejection of voluntary recommendations has also extended into the Internet of Things. The Commission brought its first Internet of Things-related case in 2013, against the manufacturer of baby monitors that had been hacked.[88] Since then, the Commission has already begun promulgating best practices for the Internet of Things, which it defines as "devices or sensors – other than computers, smartphones, or tablets – that connect, store or transmit information with or between each other via the Internet."[89] Experts believe that the Internet of Things will more than quadruple in size in the next five years, and market pressures will

---

[85] *See supra* Section I.A (discussing statistics related to recent data breaches in the United States).
[86] Pullen, *Supra* note 24.
[87] *2012 Data Breach Investigations Report*, VERIZON 3 (2012), http://www.verizonenterprise.com/resources/reports/rp_data-breach-investigations-report-2012-ebk_en_xg.pdf.
[88] Fed. Trade Comm'n, 2013 Privacy and Data Security Update 3-4 (2013), https://www.ftc.gov/system/files/documents/reports/privacy-data-security-update-2013/privacydatasecurityupdate_2013.pdf. The case was settled later that year, with the defendant agreeing to implement a "comprehensive information security program." Fed. Trade Comm'n, *Marketer of Internet-Connected Home Security Video Cameras Settles FTC Charges It Failed to Protect Consumers' Privacy* (Sep. 4, 2013), https://www.ftc.gov/news-events/press-releases/2013/09/marketer-internet-connected-home-security-video-cameras-settles.
[89] Fed. Trade Comm'n, FTC Report on Internet of Things Urges Companies to Adopt Best Practices to Address Consumer Privacy and Security Risks (Jan. 27, 2015), https://www.ftc.gov/news-events/press-releases/2015/01/ftc-report-internet-things-urges-companies-adopt-best-practices.

inevitably disincentivize producers and developers from prioritizing time-consuming cybersecurity practices, which could delay time to market.[90] This new industry is exploding, and according to a recent study by Hewlett Packard, 90% of these devices "collected at least one piece of personal information," and 70% failed to encrypt internet and network communications.[91] These security concerns are already a reality, and manufacturers have proven that they will not waste time and resources implementing voluntary data security standards. With the Internet of Things growing to include everything from household appliances and baby monitors to automobiles, the risk associated with any data breaches or hacks extends far beyond the mere loss of consumer financial information. Imagine the safety implications of exposed baby monitor video feeds, or automobile GPS information that notifies intruders when you are not home. This risk must be mitigated by some system of mandatory standards.

In light of the leading expert predictions, corporate failure to meet voluntary security standards, the future implications of the massively expanding Internet of Things, and the billions of dollars already lost as a result of data breaches, it is crucial for the federal government to be able to implement mandatory corporate cybersecurity standards in order to protect consumers and the United States from future economic and non-economic losses.

B. Wyndham *is Not a Permanent Solution to the Problem.*

The narrow holding in *Wyndham* is an insufficient solution to the corporate cybersecurity regulation problem due to the limiting factors related to the holding, and the fact that the Commission still does not have the authority to make companies adopt fair information security

[90] *2015 Data Breach Investigations Report*, VERIZON 62-63 (2015), http://www.verizonenterprise.com/DBIR/2015/.
[91] *Internet of things research study 2015 report*, HEWLETT PACKARD ENTERPRISE, 4-5 (2015), http://h20195.www2.hp.com/V2/GetDocument.aspx?docname=4AA5-4759ENW&cc=us&lc=en.

policies. This section will outline the factors that potentially limit the holding in *Wyndham*. Then it will explain how the Commission's authority is still limited after this holding.

The decision on appeal related solely to the unfairness claim brought by the Commission, and the decision by the court was limited by a number of factors present in the case. These include (1) the complete lack of a cybersecurity system, (2) the affirmative misrepresentations made by Wyndham, and (3) the foreseeability of the harm involved. First, regarding the deficiency of the cybersecurity system, due to the extreme inadequacy of Wyndham's system, it is not clear where future courts may draw the line as to what constitutes an "unfair practice" under the *Wyndham* decision. This particular case did not merely involve an inadequate cybersecurity system—there was *no* cybersecurity system in place.[92] Even the appellate court decision expressly qualified its ruling regarding fair notice on this point –

> Wyndham's as-applied challenge falls well short given the allegations in the FTC's complaint. As the FTC points out in its brief, the complaint does not allege that Wyndham used weak firewalls, IP address restrictions, encryption software, and passwords. Rather, it alleges that Wyndham failed to use any firewall at critical network points, did not restrict specific IP addresses at all, did not use any encryption for certain customer files, and did not require some users to change their default or factory-setting passwords at all.[93]

Under this decision, a future court could determine that the Commission's interpretation of "unfair" may not satisfy fair notice requirements if applied against a company with a weak cybersecurity system in place, as opposed to no system at all.

Second, in this case, Wyndham had made an affirmative misrepresentation to consumers about security of information by including in its privacy policy specific security measures it claimed to have in place.[94] It is not clear how this limitation in the facts of the case impacted the

[92] *Wyndham* at 256.
[93] *Id.* (Internal citations omitted).
[94] *Id.* at 241.

holding, but it could be used to distinguish this claim from others not involving such fraudulent activity.

Third, Wyndham's breach was clearly foreseeable, as the Court commented: "For good reason, Wyndham does not argue that the cybersecurity intrusions were unforeseeable. That would be particularly implausible as to the second and third attacks."[95] Wyndham had suffered three breaches, two using the same security weakness.[96] This limiting factor could further distinguish the *Wyndham* holding from future cases where harm was not foreseeable due to repeated attacks on a system, and known, exploited system weaknesses that the company failed to repair. Furthermore, the decision currently only applies in the Third Circuit. Other circuits are not bound by this precedent, and they may not interpret the Commission's authority in the same way.

Even if the holding in *Wyndham* were not limited by these factors, the holding still leaves the Commission unable to establish formal prophylactic regulations or preventive corporate cybersecurity standards. Although the Commission has made a substantial effort to help guide companies through the efforts outlined above,[97] it still lacks the authority to make any of these suggested security measures mandatory. The Commission has asked Congress to pass federal legislation requiring companies to implement reasonable data security policies and procedures, and delegate to the Commission the corresponding rulemaking authority.[98] The Commission has

[95] *Wyndham* at 246.
[96] *Id.* at 241-42.
[97] *Supra* Section I.C.ii.
[98] Fed. Trade Comm'n, Press Release, FTC Testifies on Data Security (June 15, 2011), https://www.ftc.gov/news-events/press-releases/2011/06/ftc-testifies-data-security. While it is not clear why Congress has failed to enact such legislation, White House Press Secretary Jay Carney has speculated that "the politics of obstructionism, driven by special interest groups seeking to avoid accountability, prevented Congress from passing legislation to better protect our nation from potentially catastrophic cyber-attacks." Ramsey Cox & Jennifer Martinez, Cybersecurity Act fails Senate vote, THE HILL (Aug. 2, 2012), http://thehill.com/policy/technology/241851-cybersecurity-act-fails-to-advance-in-senate.

acknowledged that it cannot require companies to adopt "fair information practice policies."[99] While the Commission has discretionary rulemaking authority with regard to what constitutes "unfair" or "deceptive" trade practices, this is not the type of rulemaking authority that it needs in order to adequately protect consumers. This authority is still merely remedial and only gives the Commission enforcement authority when a company has already engaged in unfair or deceptive practices. In *Wyndham*, the Court even acknowledged that the Commission does not have the authority to require companies to adopt broad fair information practice policies, however, those limitations on authority did not impact the issue in this case.[100]

Wyndham is undoubtedly a great step towards strengthening consumer protection from unreasonable data security practices in the United States; however, the decision leaves unanswered many questions regarding the FTC's authority. Additionally, as the Commission has asserted, the power recognized under this decision is still not enough to properly regulate corporate cybersecurity standards in this country.

The current regulatory framework is yet more problematic for two important policy reasons. First, the wide variety of modes of liability puts the burden of consumer protection on the already overloaded court system. Second, it fails to take steps to actually protect consumer information—all of these laws merely provide remedies where damage has already been done. This purely remedial approach has allowed data breaches to occur with increasing frequency, and has failed to protect personal information from initial exposure. While some scholarship argues that increasing consumer rights and remedies would be a step in the right direction,[101] experience

[99] *See* Fed. Trade Comm'n, Privacy Online: Fair Information Practices in the Electronic Marketplace: A Federal Trade Commission Report to Congress 34 (2000), https://www.ftc.gov/reports/privacy-online-fair-information-practices-electronic-marketplace-federal-trade-commission
[100] *Wyndham* at 248-49.
[101] *See* Simpson, Note, UNIV. COLO. L. REV. [pp] (arguing for increased individual consumer rights and remedies for data breaches).

suggests otherwise. As discussed above, companies are already at great risk for liability in the event of a data breach, and yet most still choose to not implement reasonable security practices. This failure to adopt voluntary security practices, combined with the continually increasing frequency of data breaches, and the limitations of the FTC's post-*Wyndham* authority all strongly indicate that the country's attempts to solve this problem through remedial efforts are inadequate. Implementation of additional remedial measures would likely do little to protect consumer information from initial exposure or incentivize companies to adopt improved cybersecurity practices. This leaves a significant gap in a vital area of regulation: preventing breaches from happening in the first place.

III. CONGRESS SHOULD ENACT LEGISLATION DIRECTLY ADDRESSING CORPORATE CYBERSECURITY STANDARDS

The breadth and frequency of large-scale hacks, the failure of most small businesses to implement data security plans, and the inexcusable insecurity of the products being introduced to the Internet of Things serve as strong evidence that the current limited regulatory authority with focus on punitive remedial measures is not working and needs to be overhauled. The risks and potential liability exposure for companies that fail to implement reasonable security measures have not served as a deterrent. Prophylactic legislation would shift the liability from an obscure future possibility to an immediate danger to these companies. While *Wyndham* has shown that the Commission may be able to expand its regulatory authority over data security practices through the judicial process, this method would be incredibly time-consuming and expensive for the Commission, and it would not guarantee that the Commission could gain the regulatory power it needs within the boundaries of its current authority. The *Wyndham* proceedings alone have been going on since June 26, 2012, and have not yet made it to trial. These lengthy, costly

proceedings waste the time of the Commission, courts, companies, and taxpayer dollars. This time-consuming process is even less desirable in light of the results of the expert predictions that a "major cyberattack" will occur within the next ten years.[102]

For these reasons, Congress needs to adopt prophylactic cybersecurity legislation that enables the federal government to set affirmative minimum standards that all companies handling consumer information must adhere to. This section will explore three routes Congress can take in enacting this legislation. Section A will discuss Congress' option to enact legislation directly creating specific rules and argue that this method is not desirable because such rules would be inflexible and do not grant the Commission power to require companies to adopt cybersecurity plans. Section B will discuss Congress' second option, to expand the FTCA to clarify the Commission's enforcement authority over data security, and will argue that this would be no better than our current framework, which has already proven to be insufficient. Section C will argue that the third option, to enact legislation delegating APA rulemaking authority to the Commission, is superior because it would give the Commission prophylactic rulemaking power sufficient to require companies to implement data security plans so as to maximize protection of consumer information. It would also allow the Commission to quickly implement and retire rules as technology evolves.

A. Option 1: Creating Statutory Corporate Cybersecurity Standards

One available solution to the lack of corporate cybersecurity standards is for Congress to pass legislation directly creating such standards. Indeed, Congress has attempted to pass specific legislation governing this area of law, including uniform data breach notification

[102] *Supra* note 64.

requirements,[103] and even a Consumer Bill of Rights.[104] While bills such as these, promulgating fixed rules to be enforced by an administrative agency, may be helpful in many respects, they are not an ideal solution for a variety of reasons. First, rules in this form are fixed as passed by Congress, and thus do not have the ability to evolve alongside the rapidly changing technological landscape.[105] Additionally, Congress has failed to pass many of them into law, they are often narrow in focus and not applicable to the growing Internet of Things, and they fail to take action to prevent loss of consumer information before it happens.

While certain features, such as uniform data breach notification rules that pre-empt state laws, would be helpful for companies trying to navigate the complicated state regulatory system, these proposed laws do not go far enough to protect consumers from initial exposure of their personal information. Such legislation is akin to trying to fix a flooding kitchen by soaking up the water with towels without first turning off the faucet. In order to further the interests of consumer protection and national security, a comprehensive solution should attempt to stop breaches from occurring in the first place, and should be dynamic and able to evolve with technology to avoid unreasonable delays waiting for new legislation.

B. Option 2: Expanding the FTCA to Encompass Cybersecurity Practices

Some scholars argue that Congress should simply amend the FTCA in order to clarify that the Commission has enforcement authority over information security.[106] However, this

---

[103] Data Security and Breach Notification Act of 2015, H.R. 1770, 114th Cong. (2015), https://www.congress.gov/114/bills/hr1770/BILLS-114hr1770ih.pdf.
[104] Administration Discussion Draft: Consumer Privacy Bill of Rights Act of 2015, THE WHITE HOUSE (2015), https://www.whitehouse.gov/sites/default/files/omb/legislative/letters/cpbr-act-of-2015-discussion-draft.pdf.
[105] *See* Shawn Zeller, *Congress Struggles to Keep Pace with Advances in Tech*, GOVERNMENT TECHNOLOGY (SEPT. 16, 2015), http://www.govtech.com/federal/Congress-Struggles-to-Keep-Pace-with-Advances-in-Tech.html (describing the challenges Congress has faced trying to keep up with technological change, stating "[a]dvances in the tech world are coming so fast that Congress' deliberative system can't keep pace").
[106] *See* Amanda R. Moncada, *When A Data Breach Comes A-Knockin', the FTC Comes A-Blockin': Extending the FTC's Authority to Cover Data-Security Breaches*, 64 DEPAUL L. REV. 911, 915 (2015); *see also* Simpson, 87 UNIV. COLO. L. REV. at [39].

approach is insufficient for a number of reasons. First, expansion of the FTCA would merely affirm the Commission's current enforcement authority, as dictated in *Wyndham,* and fails to provide any prophylactic regulatory authority to the agency. Expansion of the FTCA in this manner would provide no greater regulatory power than the Commission already has under the Third Circuit's interpretation of the FTCA in *Wyndham*. Further, this approach is not ideal because the Commission's focus on going after the biggest players under the FTCA would leave others effectively unregulated. Additionally, if Congress merely expanded the Commission's authority under the FTCA, it would fail to create a uniform system of laws that could fix the disjointed, contradictory state regulatory framework that to which companies are currently subjected.

Moreover, expansion of the FTCA is not an appropriate solution because of the additional impediments to effective governance of cybersecurity practices created by the heightened Magnuson-Moss rulemaking procedures.[107] Under this heightened procedural requirement, the Commission can only prescribe "interpretive rules and general statements of policy" with respect to unfair or deceptive practices, and "rules which define with specificity" what constitutes an unfair or deceptive practice.[108] Even the *Wyndham* court characterized the Magnuson-Moss procedures that the Commission is normally subject to as "burdensome."[109] In fact, the Commission has not initiated any new Magnuson-Moss rulemakings since 1980, when the procedures were modified to be even more stringent.[110] The Commission has since been forced

[107] *See* Miles W. Kirkpatrick, Joan Z. Bernstein, Robert Pitofsky, Michael F. et. al., *Report of the American Bar Association Section of Antitrust Law Special Committee to Study the Role of the Federal Trade Commission*, 58 ANTITRUST L.J. 43, 88-89 (1989) (describing Magnuson-Moss rulemaking as "a costly and uncertain tool" that some believe should be repealed).
[108] 15 U.S.C.A. § 57a (West 2012).
[109] *Wyndham* at 248.
[110] Jeffrey S. Lubbers, *It's Time to Remove the "Mossified" Procedures for FTC Rulemaking*, 83 GEO. WASH. L. REV. 1979, 1989 (2015).

to try to regulate alternatively through non-binding guidelines, and it has only successfully promulgated new rules where Congress has granted through legislation explicit APA rulemaking authority in a particular area.[111] This type of explicit APA rulemaking authority is necessary for the Commission to effectively regulate corporate cybersecurity standards.

C. Option 3: Enacting Legislation Delegating to the Commission Administrative Procedure Act Rulemaking Authority over Corporate Cybersecurity Practices

Legislation enabling the Commission to establish flexible prophylactic rules regarding corporate cybersecurity standards is the only effective means of regulating corporate data security practices. This Section will argue that Congress should pass legislation granting the Commission APA rulemaking authority to promulgate and enforce reasonable information security standards for all companies using, storing, and transmitting consumer personal and financial information, including information transmitted via products within the Internet of Things.

Congress' approach must embrace a flexible rulemaking element in order to effectively govern corporate cybersecurity practices. Technology is rapidly evolving; legislating is an ossified process. By the time Congress passes a law to react to the technology of yesterday, many new problems will likely have already arisen that escape the boundaries of that legislation. Over the past eight years, Congress has only managed to enact between one and three percent of the overall legislation presented to it, a marked decrease from prior years.[112] Additionally, those cybersecurity bills that are eventually enacted can take over a year to be passed from the time

[111] *Id.*at 1989-90.
[112] *Statistics and Historical Comparisons*, Govtrack.us (last visited Nov. 15, 2015), https://www.govtrack.us/congress/bills/statistics.

they are introduced.[113] The federal government needs to adopt an approach that allows quick promulgation and enforcement of rules that can react to cybersecurity issues as they arise and also allows for retirement of rules when they become irrelevant or burdensome. FTC Commissioner, Edith Ramirez, stressed this point in a Senate Commerce Committee hearing on information security legislation, characterizing this flexibility as a "critically important" component of any legislation that Congress decides to enact.[114] Although some agencies have notoriously taken years to pass regulations,[115] statistics show this would likely not be the case with the Commission. When granted APA rulemaking authority over a specific area, the median time required for the Commission to issue a rule is 190 days.[116]

Furthermore, prophylactic rulemaking authority is the critical piece of this proposal that differentiates this legislation from the current regulatory framework. In order to cut data breaches off at the source, Congress must grant the Commission the authority to affirmatively require companies to adopt data security plans before consumer information is put at risk. Given that 97% of data breaches in 2011 were avoidable with simple or intermediate security controls, this authority to make corporate cybersecurity plans mandatory could serve to eliminate almost all data breaches.[117]

As discussed above, the Commission has already taken ownership of data security by promoting business and consumer education, promulgating guidelines and best practices, and

---

[113] *See* Cybersecurity Enhancement Act of 2014 Actions Overview, Congress.gov (Last visited Nov. 15, 2015), https://www.congress.gov/bill/113th-congress/senate-bill/1353/actions?q={%22search%22%3A[%22\%22Cybersecurity+Enhancement+Act+of+2014\%22%22]}&resultIndex=1.

[114] Andrew Scurria, *FTC Wants Rulemaking Power for Cybersecurity Reforms*, LAW360 (Mar 26, 2014), http://www.law360.com/articles/521665/ftc-wants-rulemaking-power-for-cybersecurity-reforms.

[115] *See, e.g. Pub. Citizen Health Research Grp. v. Chao*, 314 F.3d 143 (3d Cir. 2002) (describing as excessive OSHA's 9 year delay in promulgating a new rule regarding Hexavalent Chromium).

[116] Lubbers, 83 GEO. WASH. L. REV. at 1995-96.

[117] *2012 Data Breach Investigations Report*, VERIZON 3 (2012), http://www.verizonenterprise.com/resources/reports/rp_data-breach-investigations-report-2012-ebk_en_xg.pdf.

traveling around the country to better educate business on implementing better security plans, making it the ideal candidate for this cybersecurity regulatory authority. The Commission has clearly devoted a lot of time and resources to this issue, has developed subject-matter expertise, and is in a good position to begin enforcement activities.

This law would also further public policy goals by reducing the amount of litigation crowding the court dockets. Moreover, it would facilitate establishment of a bright line rule that would reduce confusion for the inevitable borderline cases, where a company's cybersecurity practices tread very close to the line of unfair.[118] Furthermore, this approach would (1) enable quick implementation of policies due to the Commission's already-established subject-matter expertise; (2) increase protection of consumer information; (3) decrease the number of data breaches that occur; (4) consolidate a complicated state regulatory framework into a workable, uniform rule for all companies subject to data security laws; (5) provide an additional line of defense against cybercrime in the United States; and (6) allow the Commission APA rulemaking authority, thus escaping the heightened notice-and-comment rulemaking requirements of the Magnuson-Moss Act that would apply to any expansion of the authority under the FTCA. Authority to create rules under the standard notice-and-comment procedures within the APA would enable the Commission to more effectively govern this area of law without stumbling over outdated and increasingly obstructionist road blocks.

The Commission has a variety of tools in its toolbox in order to formulate a rule that would effectively address concerns of a wide variety of businesses. It could adapt the NIST framework into a workable mandatory baseline, requiring companies handling consumer information and devices within the Internet of Things to develop and implement policies and

[118] *See F.T.C. v. Wyndham Worldwide Corp*, 799 F.3d 236, 256-57 (2015) ("We acknowledge there will be borderline cases where it is unclear if a particular company's conduct falls below the requisite legal threshold").

procedures that follow the NIST's five primary functions of cybersecurity systems. That a number of private entities have already begun to look to the NIST standards as a de facto framework illustrates their viability as mandatory requirements and their suitability for corporate interests.[119] The Commission has also already used its expertise to publish best practices that could be used to guide companies through implementation of a mandatory data security plan.[120]

Furthermore, the Commission could issue standards applicable to all devices connected to the Internet of Things. A 2015 Commission report suggested that Internet of Things companies should incorporate security into their design process by, "(1) conducting a privacy or security risk assessment; (2) minimizing the data they collect and retain; and (3) testing their security measures before launching their products."[121] The Commission could easily transform this suggestion into a requirement, immediately reducing the security risk posed by these devices. As further suggested in this report, companies engaged in developing or maintaining Internet of Things-related devices and underlying technology should also be required to implement mandatory employee training on information security.[122] Additional safeguards should include a mandatory risk-assessment policy and procedures designed to alert a company of any vulnerabilities.

Inevitably, such far-reaching regulatory authority will garner objections from companies who want to avoid government intrusion on private company internal practices. A possible compromise, already utilized by the Commission in some settlement agreements, is to require

---

[119] NIST Cybersecurity Framework, *supra* note 29.
[120] Fed. Trade Comm'n, FTC Issues Final Commission Report on Protecting Consumer Privacy, (Mar. 26, 2012), https://www.ftc.gov/news-events/press-releases/2012/03/ftc-issues-final-commission-report-protecting-consumer-privacy.
[121] Fed. Trade Comm'n, Internet of Things: Privacy & Security in a Connected World iii (2015), https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf.
[122] *Id.*

independent cybersecurity auditing.[123] Such independent auditing would require submission of bi-annual audit reports. This would be an ideal approach to satisfy the interest of all parties involved—it would keep government out of companies' private information, while simultaneously enabling effective regulation of cybersecurity practices. This auditing requirement would also serve to ensure that all companies falling within the purview of the Commission's cybersecurity oversight authority are regularly monitoring cybersecurity practices. Given the vast number of companies such standards would apply to, an independent audit framework would further serve to alleviate the Commission's burden of enforcing these standards.

There is also a possibility that laws governing security of consumer information could inhibit innovation and economic growth by setting standards that are too expensive for smaller companies to comply with. However, this concern must be balanced against the greater public policies of national security and consumer protection. Moreover, though the cost of implementing cybersecurity measures may be relatively high, such measures will prevent a wide variety of other expenses that would result from a data breach, including mandatory post-breach processes,[124] direct economic losses, exorbitant litigation costs, reputational loss, and the subsequent expense of implementing data security measures to prevent any future data breaches.

A basic cost-benefit analysis indicates that the expenses incurred by a smaller company for data security are much less than the cost of a data breach. Even the most minor data breach, resulting in the loss of a mere 100 records, will likely cause an organization to lose between

---

[123] *See supra* note 14.

[124] *See* Bill Carey, *Take Security Seriously, Avoid Cost of Breaches*, BUSINESS NEWS DAILY (Feb. 11, 2013), http://www.businessnewsdaily.com/3933-security-tips-small-businesses.html (estimating the average small business expense for mandatory post-breach processes at $200,000, including the cost of notifying customers, hiring outside experts to determine what went wrong, and identifying company obligations after the breach).

$18,000 and $36,000.[125] The average loss for a breach of 1,000 records is forecast to be between $52,000 and $87,000.[126] The numbers increase from there.[127] The risk of loss for small businesses is even worse—almost two-thirds are forced to close their doors within six months of suffering a data breach.[128] An outsourced cybersecurity system can cost around $57,000 for a 50-employee company.[129] However, this estimate is deceptively high, as it includes expenses for services a company is likely already using, including email and phone services, and salaries for outsourced IT workers which may not be necessary.[130] Given that the vast majority of U.S. organizations have experienced data breaches,[131] it follows that the benefit gained by implementing proper cybersecurity practices outweighs the cost, and even without mandatory federal regulations, cybersecurity systems should be incorporated as a necessary expense of operating business in the twenty-first century.

CONCLUSION

The Commission has made huge advances over the last fourteen years in the area of data security enforcement in the absence of any federal legislation. Without the Commission's efforts, the nation's consumers would be left with no federal protection against the exposure of personal and financial information by companies failing to implement reasonable data security practices. However, as technology evolves and the ability to opt out of disclosing personal information to companies disappears, the federal government's need to strengthen consumer protection against data exposure grows.

---

[125] Verizon, *supra* note 90 at 30.
[126] *Id*.
[127] *Id*.
[128] Pullen, *Supra* note 24.
[129] Patrick Clark, *The Bill for Cybersecurity: $57,600 a Year*, BLOOMBERG (Oct. 31, 2014), http://www.bloomberg.com/bw/articles/2014-10-31/cybersecurity-how-much-should-it-cost-your-small-business.
[130] *Id*.
[131] *See The Liability of Technology Companies for Data Breaches* 3, *supra* note 26.

The current legislative framework focuses on a punitive and remedial approach that is not working, and has resulted in the loss of billions of dollars in recent years. Although *Wyndham* is a step in the right direction, the current piecemeal cybersecurity regulatory system still needs an overhaul. In addition to the ongoing financial risks posed to consumers by companies that have suffered data breaches, the rapid growth of the Internet of Things poses substantially more serious risks, including public safety and cyberattacks, which need to be addressed. Congress should adopt prophylactic federal legislation allowing the Commission to directly regulate corporate cybersecurity standards in order to prevent future data breaches and loss of personal information before they happen.