HOW TO PROTECT CONSUMER DATA? LEAVE IT TO THE CONSUMER PROTECTION AGENCY: FTC RULEMAKING AS A PATH TO FEDERAL CYBERSECURITY REGULATION

Hayes Hagan*

In the wake of cases challenging the scope of the Federal Trade Commission's authority and its role in regulating cybersecurity, this Note considers the centrality of the FTC as a protector of consumer data. It broadly examines the current state of cybersecurity regulation and the need for a uniform national regime to protect consumer data. In considering different methods for realizing such federal oversight, this Note examines legislative and administrative options. Tracing the development of both highlights their shortcomings and reveals a potential solution. In the face of concerning legislative movement and uncertainty surrounding the FTC's current enforcement philosophy, this Note endorses the employment of the FTC's rarely used, but highly effective, rulemaking authority as a tool to complement and enhance its adjudicative enforcement.

* J.D. Candidate 2020, Columbia Law School; B.S. & B.B.A. 2017, University of Kentucky. The author is sincerely grateful to Joseph DeMarco for his invaluable comments and guidance on this Note. Additional thanks to Caelainn Carney, Andrew Astore, and the staff of the *Columbia Business Law Review* for their editing and assistance in preparing this Note for publication.

I. INTRODUCTION

The growing connectivity of the world and the deepening reliance on digital platforms give rise to many new threats.[1] As inexpensive electronic storage has grown more available, the volume of data created and stored has exploded.[2] This presents a growing security risk, as the value of that data invites theft.[3] Indeed, since the rise of inexpensive electronic storage, cyberattacks and data breaches have increased dramatically in frequency and magnitude.[4]

This Note examines potential methods of addressing this issue. Specifically, it highlights the need for federal

[1] *See* SYMANTEC, INTERNET SECURITY THREAT REPORT 5 (2018), https://www.symantec.com/content/dam/symantec/docs/reports/istr-23-2018-en.pdf [https://perma.cc/367P-PJJV]; *see also* Martin Giles, *Six Cyber Threats to Really Worry About in 2018*, MIT TECH. REV. (Jan. 2, 2018), https://www.technologyreview.com/s/609641/six-cyber-threats-to-really-worry-about-in-2018/ [https://perma.cc/9QX7-Q24F].

[2] *See* MCKINSEY GLOB. INST., THE AGE OF ANALYTICS: COMPETING IN A DATA-DRIVEN WORLD 1 (2016), https://www.mckinsey.com/~/media/McKinsey/Business%20Functions/McKinsey%20Analytics/Our%20Insights/The%20age%20of%20analytics%20Competing%20in%20a%20data%20driven%20world/MGI-The-Age-of-Analytics-Full-report.ashx [https://perma.cc/HS99-2W88].

[3] *See generally* Taylor Armerding, *The 18 Biggest Data Breaches of the 21st Century*, CSO (Dec. 20, 2018), https://www.csoonline.com/article/2130877/data-breach/the-biggest-data-breaches-of-the-21st-century.html [https://perma.cc/887Z-PWQ2].

[4] *See* PONEMON INST., 2018 COST OF A DATA BREACH STUDY: GLOBAL OVERVIEW 3, 23 (2018). https://databreachcalculator.mybluemix.net/assets/2018_Global_Cost_of_a_Data_Breach_Report.pdf [https://perma.cc/8D7B-WFM6].

regulation, explores how such a regulatory scheme may be feasibly implemented, and outlines the form such regulation should take.

In the wake of cases challenging the role of the Federal Trade Commission (the "FTC" or "Commission") and the scope of its authority in regulating cybersecurity, this Note considers the centrality of the FTC as a protector of consumer data. It also endorses the use of the FTC's rarely exercised, but highly effective, rulemaking authority as a tool to complement and enhance its adjudicative enforcement.

Part II offers a brief overview of the current state of regulation and reveals the need for federal intervention. It discusses the duplicative and inconsistent state regulations and exposes the gap left by the existing federal regulations, which are largely industry-specific and leave vast amounts of data unprotected. It then explores the legislative and administrative avenues available for federal regulation. Tracing the stagnant, years-long process of passing cybersecurity legislation, this Note demonstrates the need to pursue an alternative path for federal regulation. As large technology companies exercise their political muscle to lobby for regulation themselves,[5] this Note cautions against premature celebration and investigates their intentions. Like the lobbying of tobacco companies in the 1960s, such efforts may be thinly veiled attempts to preempt more meaningful regulation.[6]

Looking to the administrative avenue of federal regulation, this Note examines the extent to which various agencies regulate cybersecurity and identifies the gap that has allowed the most recent, well-publicized data breaches to occur. It

[5] *See infra* Section II.A.

[6] When faced with the prospect of unfavorable regulations, Big Tobacco made concerted efforts to preempt them by advancing and supporting their own, more palatable, federal laws. *See* Elizabeth Drew, *The Quiet Victory of the Cigarette Lobby: How It Found the Best Filter Yet—Congress*, ATLANTIC, Sept. 1965, https://www.theatlantic.com/magazine/archive/1965/09/the-quiet-victory-of-the-cigarette-lobby-how-it-found-the-best-filter-yet-congress/304762/ [https://perma.cc/J9VP-TC2Z].

then discusses the unique position of the FTC and why it is best situated to fill this gap.

Part III provides an in-depth look at the FTC's role as a cybersecurity regulator. It briefly surveys the Commission's history of enforcement and summarizes two recent cases, *FTC v. Wyndham Worldwide Corp.*[7] and *LabMD, Inc. v. FTC*,[8] which challenged—and, in their resolution, somewhat crystallized—the scope of the FTC's authority to regulate cybersecurity. Reviewing this history reveals the drawbacks of enforcement through adjudication. In response, this Note considers how to overcome these weaknesses and how the FTC can complement its enforcement efforts with other available tools to optimize its overall effectiveness.

Part III then proposes the FTC invoke its relatively dormant rulemaking authority. Promulgating a rule would serve as notice to all companies and give teeth to any subsequent adjudication by allowing the FTC to seek meaningful penalties. There is, however, good reason the FTC has not tried using this authority yet, and this Note outlines the unique obstacles presented by the particularly convoluted procedure the FTC would be subject to. Revisiting Congress's purpose in imposing these procedural requirements, this Note argues that Congress should allow a specific exception so the FTC can address the growing threat of cyberattacks, as it did with the Children's Online Privacy Protection Rule, the Privacy of Consumer Financial Information rule, and the Health Breach Notification Rule.[9]

Part IV offers a path forward in light of the aforementioned obstacles. Amid calls for legislation, which carries the risk of overvaluing the interests of large companies, Congress can instead grant streamlined rulemaking authority to the FTC. The FTC can establish rules that both protect consumers and

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

[8] LabMD, Inc. v. FTC, 894 F.3d 1221 (11th Cir. 2018).

[9] These rules were passed after Congress allowed specific exceptions for the FTC to use a streamlined rulemaking process. *See* Children's Online Privacy Protection Rule, 16 C.F.R. § 312 (2018); Privacy of Consumer Financial Information, 16 C.F.R. § 313 (2018); Health Breach Notification Rule, 16 C.F.R. § 318 (2018).

complement its adjudicative efforts. This solution fills the gap in current regulation while sidestepping the pitfalls of other approaches.

II. AVENUES TO FEDERAL REGULATION

Currently, state privacy laws provide the most comprehensive domestic regulation of American consumers' data, but federal action is necessary. While Congress has failed to enact sweeping legislation governing all businesses that collect consumer data,[10] state governments have acted to protect their residents.[11] Since Alabama and South Dakota passed laws last year, all fifty states, together with the District of Columbia, Guam, Puerto Rico, and the United States Virgin Islands, have passed data breach notification laws.[12]

These state laws afford some protection to consumers, but they simply cannot provide the simplicity and comprehensiveness of federal regulation.[13] Indeed, the current legal landscape is a patchwork quilt of varying definitions and requirements. The lack of uniformity creates a costly headache for companies trying to ensure compliance.[14] As it stands, the state laws in effect are far from transposed copies of the same legislation. They differ in their

[10] *See* Nuala O'Connor, *Reforming the U.S. Approach to Data Protection and Privacy,* COUNCIL ON FOREIGN REL. (Jan. 30, 2018), https://www.cfr.org/report/reforming-us-approach-data-protection [https://perma.cc/CRD2-7GMN].

[11] *See Security Breach Notification Laws*, NAT'L CONF. ST. LEGISLATURES (Sept. 29, 2018), http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx [https://perma.cc/A8V8-LRHA].

[12] *See id.*

[13] *See generally* Jacqueline May Tom, Note, *A Simple Compromise: The Need for a Federal Data Breach Notification Law*, 84 ST. JOHN'S L. REV. 1569, 1571 (2010).

[14] *See, e.g.*, Kate Fazzini, *Goldman's Top Cybersecurity Official Complains About Patchwork of Laws*, *Says He Spends Too Much Time Talking to Regulators,* CNBC (Dec. 11, 2018), https://www.cnbc.com/2018/12/11/goldman-sachs-cisoandy-ozment-complains-about-patchwork-of-laws.html [https://perma.cc/HE6F-9WKQ].

definition of what constitutes sensitive personal information; what qualifies as a breach; when, to whom, and how disclosure is required; and whether any exceptions or safe harbors exist.[15] Companies can conservatively comply with all state statutes, but the resulting over-compliance is costly and may lead to reputational harm and a competitive disadvantage.[16] Complying with different laws also requires companies to keep abreast of all the applicable laws and amendments of every state, each having its own variations.[17] This requires a great deal of time and effort and "[i]n most cases, looking up each of the . . . statutes one by one is the only way to fully understand the differences."[18]

Technology will inevitably continue to evolve, but laws surrounding breaches need not change substantially in response to justify the current patchwork of conflicting state laws. Aside from updating what constitutes a breach or incident, details like the time period for notification, who companies must report them to, and what constitutes personally identifiable information should not require frequent adjustments. A unified federal regulatory scheme could resolve many of the issues created by the existing regime. Such a federal cybersecurity regime could be created through legislation, administrative action, or some combination of the two.

A. Legislative Avenue

While the United States has been slow to establish a national data privacy regime, many other countries and regions have implemented their own. The governments of Canada, Australia, and the European Union ("EU") have all

[15] *See generally* PERKINS COIE, SECURITY BREACH NOTIFICATION CHART (June 2018), https://www.perkinscoie.com/images/content/1/9/v2/197566/Security-Breach-Notification-Law-Chart-June-2018.pdf [https://perma.cc/GPH3-WA5P].

[16] *See* Tom, *supra* note 13, at 1571.

[17] *See id.* at 1570.

[18] *Id.*

enacted comprehensive data privacy legislation.[19] In fact, the EU regulation smoothly replaced its own patchwork of conventions, directives, treaties, and individual European country rules,[20] offering a model to the United States. As a result, companies quickly responded to ensure compliance.[21] While companies have loudly lamented the resulting cost,[22] according to the 2018 Thales Data Threat Report, seventy-four percent of respondents in the United States and sixty-four percent around the world feel that adhering to compliance standards is a "very" or "extremely" effective way to keep sensitive data secure.[23] Besides, while the upfront costs may be apparent, compliance is very likely a cost-saver in the long run. Considering more than half of U.S. businesses

[19] *See* Personal Information Protection and Electronic Documents Act, S.C. 2000, c 5 (Can.); *Privacy Amendment (Notifiable Data Breaches) Act 2017* (Cth) (Austl.); Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation), 2016 O.J. (L 119) 1.

[20] *See* Christina Glon, *Data Protection in the European Union: A Closer Look at the Current Patchwork of Data Protection Laws and the Proposed Reform That Could Replace Them All*, 42 INT'L J. LEGAL INFO. 471, 472 (2014).

[21] *See* Adam Satariano, *G.D.P.R., a New Privacy Law, Makes Europe World's Leading Tech Watchdog*, N.Y. TIMES (May 24, 2018), https://www.nytimes.com/2018/05/24/technology/europe-gdpr-privacy.html [https://perma.cc/34PC-T8WG] ("The notices are flooding people's inboxes en masse, from large technology companies . . . . 'Here is an update to our privacy policy,' they say. . . . All are acting because the European Union on Friday enacts the world's toughest rules to protect people's online data.").

[22] *See* Jeremy Kahn, Stephanie Bodoni & Stefan Nicola, *It'll Cost Billions for Companies to Comply with Europe's New Data Law*, BLOOMBERG BUSINESSWEEK (Mar. 22, 2018), https://www.bloomberg.com/news/articles/2018-03-22/it-ll-cost-billions-for-companies-to-comply-with-europe-s-new-data-law (on file with the *Columbia Business Law Review*).

[23] *See* THALES & 451 RES., 2018 THALES DATA THREAT REPORT 15 (2018), https://www.thalesesecurity.com/2019/data-threat-report [https://perma.cc/7NLP-VLKZ].

experienced a cyberattack in 2017 alone[24] and the average cost of a breach to companies is $3.86 million,[25] the investment in cybersecurity—whether mandated or not—may more than pay for itself. This is not to mention the avoided costs of penalties added by new legislation or the more insidious costs borne by consumers who are exposed to identity theft. A recent Department of Justice ("DOJ") study found that identity theft costs each victim an average of $1343, including direct financial loss and indirect costs such as legal fees and overdraft charges.[26]

Yet, regulation has stalled in the United States at the federal level. Although Congress passed laws to protect financial information,[27] healthcare information,[28] and infrastructure,[29] broad regulation setting a baseline for all companies that process personal data has yet to be enacted.[30] This is not for lack of effort. For over a decade, Congress has been actively trying to pass bills to protect consumer data. As early as 2005, there were "at least seven House and Senate committees working on federal legislation directly addressing what organizations should do when individuals' personal and private data has been illegally accessed."[31] Ultimately, these

[24] *See* Press Release, Munich RE, Half of U.S. Businesses Have Been Hacked (Sept. 28, 2017), https://www.munichre.com/HSB/business-hacked-survey-2017/index.html [https://perma.cc/23VG-5Z3U].

[25] PONEMON INST., *supra* note 4, at 3.

[26] ERIKA HARRELL, U.S. DEP'T OF JUSTICE, VICTIMS OF IDENTITY THEFT, 2014, at 6 (Nov. 13, 2017), https://www.bjs.gov/content/pub/pdf/vit14.pdf [https://perma.cc/4WXE-BMEC].

[27] *See* Gramm-Leach-Bliley Act, Pub. L. No. 106-102, §§ 501–510, 113 Stat. 1338, 1436–45 (1999) (codified as amended at 15 U.S.C. §§ 6801–6809 (2012)).

[28] *See* Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, § 221, 110 Stat. 1936, 2009–11 (codified as amended at 42 U.S.C. § 1320a–7e (2012)).

[29] *See generally* Federal Information Security Management Act of 2002, Pub. L. No. 107-347, §§ 301–305, 116 Stat. 2899, 2946–61.

[30] *See* O'Connor, *supra* note 10; *see also* Tom, *supra* note 13, at 1752.

[31] Samuel Lee, Note, *Breach Notification Laws: Notification Requirements and Data Safeguarding Now Apply to Everyone, Including Entrepreneurs*, 1 ENTREPRENEURIAL BUS. L.J. 125, 136 n.63 (2006) (citing Personal Data Privacy and Security Act of 2005, S. 1789, 109th Cong.

early bills were "mired down in committees by turf wars and intense lobbying."[32] Similar bills have been introduced almost every year since, all suffering the same fate.[33]

On one hand, the growing number of state and international cybersecurity regulations provide a model for Congress.[34] The burden of complying with the increasingly complex regulations could also encourage companies to embrace a national standard. However, the proliferation of some stricter state standards—such as the California Consumer Privacy Act[35]—has prompted large tech companies to begin lobbying Congress for weaker privacy regulations. The goal of the tech giants, it seems, is to nullify these stricter

(2005); Identity Theft Protection Act, S. 1408, 109th Cong. (2005); Notification of Risk to Personal Data Act, S. 1326, 109th Cong. (2005); Data Accountability and Trust Act, H.R. 4127, 109th Cong. (2005); Information Protection and Security Act, S. 500, 109th Cong. (2005); Information Protection and Security Act, H.R. 1080, 109th Cong. (2005); Financial Data Protection Act of 2005, H.R. 3997, 109th Cong. (2005); Consumer Data Notification and Security Act of 2005, H.R. 3140, 109th Cong. (2005)).

[32] Sarah Ludington, *Reining in the Data Traders: A Tort for the Misuse of Personal Information*, 66 MD. L. REV. 140, 157 (2006).

[33] *See, e.g.,* Data Accountability and Trust Act, H.R. 5388, 115th Cong. (2018); Data Security and Breach Notification Act, S. 2179, 115th Cong. (2017); Data Accountability and Trust Act, H.R. 580, 114th Cong. (2015); Data Security and Breach Notification Act of 2015, S. 177, 114th Cong. (2015); Data Accountability and Trust Act, H.R. 4400, 113th Cong. (2014); Data Security and Breach Notification Act of 2014, S. 1976, 113th Cong. (2014); Data Security and Breach Notification Act of 2013, S. 1193, 113th Cong. (2013); Data Security and Breach Notification Act of 2012, S. 3333, 112th Cong. (2012); Data Accountability and Trust Act of 2011, H.R. 1841, 112th Cong. (2011).

[34] *See* Charlotte A. Tschider, *Experimenting with Privacy: Driving Efficiency Through a State-Informed Federal Data Breach Notification and Data Protection Law*, 18 TUL. J. TECH. & INTELL. PROP. 45, 66 (2015); *see also America Should Borrow from Europe's Data-Privacy Law*, ECONOMIST (Apr. 5, 2018), https://www.economist.com/leaders/2018/04/05/america-should-borrow-from-europes-data-privacy-law [https://perma.cc/GET5-ZUEK].

[35] CAL. CIV. CODE §§ 1798.100–.199 (West 2019) (effective Jan. 1, 2020); *see also* Daisuke Wakabayashi, *California Passes Sweeping Law to Protect Online Privacy,* N.Y. TIMES (June 28, 2018), https://www.nytimes.com/2018/06/28/technology/california-online-privacy-law.html [https://perma.cc/LLA3-9DWY].

regulations and prevent them from becoming the de facto national standard.[36]

This is not the first time large businesses have attempted to escape impending safety standards by advocating for legislation on their own terms. In the 1960s, the tobacco industry, facing the prospect of federal regulation, made similar efforts to endorse tobacco-related legislation as a way to forestall heightened consumer protection requirements.[37] During that time, the FTC had recommended to Congress that consumers should be alerted of the new proven risks of smoking cigarettes.[38] Specifically, it recommended that all packages be labeled "*Caution: Cigarette Smoking Is Dangerous to Health. It May Cause Death from Cancer and Other Diseases*."[39] Initially, the tobacco industry invested heavily in lobbying to prevent such a warning label requirement.[40] But under the guidance of Abe Fortas, a future Supreme Court justice, and former Kentucky governor Earle Clements, the industry dramatically altered its strategy.[41] The tobacco makers began voluntarily requesting regulation—just as tech companies are today.[42] For the tobacco industry, the strategy proved successful. Congress passed the Federal Cigarette Labeling and Advertising Act

[36] *See* Cecilia Kang, *Tech Industry Pursues a Federal Privacy Law, on Its Own Terms*, N.Y. TIMES (Aug. 26, 2018), https://www.nytimes.com/2018/08/26/technology/tech-industry-federal-privacy-law.html [https://perma.cc/9G7K-P2BL] ("In recent months, Facebook, Google, IBM, Microsoft and others have aggressively lobbied officials in the Trump administration and elsewhere to start outlining a federal privacy law, according to administration officials and the companies. The law would have a dual purpose, they said: It would overrule the California law and instead put into place a kinder set of rules that would give the companies wide leeway over how personal digital information was handled.").

[37] *See* Drew, *supra* note 6.

[38] Unfair or Deceptive Advertising and Labelling of Cigarettes in Relation to the Health Hazards of Smoking, 29 Fed. Reg. 8303, 8324 (July 2, 1964).

[39] *Id.* at 8326.

[40] *See* Drew, supra note 6.

[41] *See id.*

[42] *See id.*

(FCLAA) of 1965, diluting the FTC's recommendation.[43] Under the FCLAA, warning labels only had to read, "Caution: Cigarette Smoking May Be Hazardous to Your Health."[44] This requirement was a step forward to be sure, but notably altered the FDA's proposed language, which stated that smoking "is dangerous", to say that it "may be hazardous" and expunged the words "death" and "cancer." Significantly, this new federal law preempted all state laws, ensuring no stronger protections could be implemented by any state.[45]

Much like the tech giants of today, tobacco makers were large economic engines that wielded significant political power thanks to generous campaign contributions and well-funded lobbying campaigns.[46] Now that California has passed legislation with strict data security requirements going into effect in 2020,[47] Big Tech appears to be following Big Tobacco's playbook. Companies like Google and Facebook are scrambling to get palatable federal legislation passed that will preempt state laws—including California's stricter standards.[48] These federal bills may promise increased consumer protection, but they will instead represent a delay to, or even a step back from, the progress made by states.

Past attempts at federal regulation of consumer data storage encountered political gridlock and inaction, while new efforts appear to be engineered by self-interested technology firms seeking to undercut the progress of newly-minted state laws—to the detriment of consumers. For consumers, the talk of federal legislative action does not necessarily translate to greater protection. However, the authority afforded to federal administrative agencies by existing mandates may provide another way to fill the void.

---

[43] *See* Federal Cigarette Labeling and Advertising Act, Pub. L. No. 89-92, 79 Stat. 282 (codified as amended at 15 U.S.C. §§ 1331–1341 (2012)).

[44] *See id.* § 4.

[45] *See id.* § 5(a)–(b); *see also* Drew, *supra* note 6.

[46] *See* Drew, *supra* note 6.

[47] CAL. CIV. CODE §§ 1798.100–.199 (West 2019) (effective Jan. 1, 2020); *see also* Wakabayashi, *supra* note 35.

[48] *See* Kang, *supra* note 36.

B. Administrative Agency Avenue

In line with the aforementioned industry-specific legislation that has passed through Congress,[49] various agencies have the authority to regulate data privacy within their respective spheres. Student data are governed by the Department of Education;[50] health data are governed by the Department of Health & Human Services;[51] banking data are governed by federal banking agencies such as the Office of the Comptroller of the Currency, the Board of Governors of the Federal Reserve System, and the Federal Deposit Insurance Corporation;[52] and data of those who trade in securities markets are governed by the Securities and Exchange Commission ("SEC").[53] The data security architecture of the federal government is complicated, but each agency is legally responsible for its own cybersecurity,[54] and agency compliance is primarily monitored by the Department of Homeland Security ("DHS").[55]

[49] *See supra* notes 27–29 and accompanying text.

[50] *See* 20 U.S.C. § 1232g (2012).

[51] *See* 42 U.S.C. § 1320d-6(2012).

[52] *See generally* Financial Services and Cybersecurity: The Federal Role, EVERYCRSREPORT.COM (Mar. 23, 2016), https://www.everycrsreport.com/reports/R44429.html [https://perma.cc/52WD-RWWE].

[53] *See* 17 C.F.R. § 248 (2019).

[54] *See* 44 U.S.C § 3554 (2012).

[55] While the specific oversight and monitoring roles are a complex web of responsibilities, the cybersecurity of the federal government itself is handled largely by the DHS (with support from internal DHS entities such as the National Cybersecurity and Communications Integration Center and the new Cybersecurity and Infrastructure Security Agency, with external support from the Department of Defense, Federal Bureau of Investigation, and National Security Agency) according to standards developed by the National Institute of Standards and Technology (within the Department of Commerce) and in line with policies promulgated by the Office of Management and Budget. *See* KATE CHARLET, HARV. KENNEDY SCHOOL BELFER CTR FOR SCI. & INT'L AFFAIRS., UNDERSTANDING FEDERAL CYBERSECURITY 8, 10–13 (2018), https://www.belfercenter.org/sites/default/files/files/publication/Understanding%20Federal%20Cybersecurity%2004-2018_0.pdf [https://perma.cc/G93J-QRAK]; *see also* Olivia Beavers, *Trump Signs Bill Cementing Cybersecurity Agency at DHS*, HILL (Nov. 16,

Recent activity in the area gives the impression that the federal government is expanding the authority of agencies to monitor civilian cybersecurity. In fact, President Trump recently signed a bill that bolsters the DHS's role in data security.[56] However, while this new law demonstrates the increased attention to and prioritization of the federal government's role in cybersecurity, it follows the pattern of sector-specific regulation, limiting its application primarily to government infrastructure.[57] It does nothing, by contrast, to advance the security of consumer data held by private institutions. In 2017, government data was the subject of only 4.7% of breaches, whereas business data accounted for 55.1% of breaches.[58] Additionally, the healthcare and banking industries—subject to the sector-specific regulations—account for only 23.7% and 8.5% of breaches, respectively.[59] This difference may be evidence of the effectiveness of current regulations, or distortions caused by under-reporting, but such a determination would require further exploration beyond the scope of this Note. This Note's primary concern is addressing the glaring issue of business sector breaches.

The SEC is working to address this issue, but its focus is limited to "federal securities laws as they apply to public operating companies."[60] Regulation of public companies satisfies some of the need for federal protection of consumer data, but it is important to remember that only 3600 firms were listed on U.S. stock exchanges at the end of 2017.[61] This

2018), https://thehill.com/policy/cybersecurity/417185-trump-signs-bill-cementing-cybersecurity-agency-at-dhs [https://perma.cc/4TB4-68SS].

56 *See* Beavers, *supra* note 55.

57 *See id.*

58 IDENTITY THEFT RES. CTR., 2017 ANNUAL DATA BREACH YEAR-END REVIEW 6 (2017), https://www.idtheftcenter.org/images/breach/2017Breaches/2017AnnualDataBreachYearEndReview.pdf [https://perma.cc/QKB3-BT8E].

59 *Id.*

60 Commission Statement and Guidance on Public Company Cybersecurity Disclosures, 83 Fed. Reg. 8165, 8166 (Feb. 26, 2018) (to be codified at 17 C.F.R pts. 229, 249).

61 Editorial, *Where Have All the Public Companies Gone?*, BLOOMBERG (Apr. 9, 2018), https://www.bloomberg.com/opinion/articles/

number represents just a fraction of a percent of the nearly twenty-eight million firms operating in the United States.[62] Unless the remainder fall under the scope of industry-specific regulations, they are not subject to any federal oversight, leaving a large swath of consumer data unprotected. The FTC, with its broad scope and general mission of consumer protection,[63] is uniquely well-situated to regulate data security for all the firms otherwise untouched by federal regulation.

III. THE FTC'S ROLE AS CYBERSECURITY REGULATOR

Compared to Congress, the FTC is better positioned to offer meaningful protection to consumer data. Although consumers would stand to benefit from such protection, large companies facing increased compliance costs have greater incentives to take a political stand against meaningful protection and have the resources to do so. In other words, the loss to an individual consumer does not justify a lobbying campaign, while the potential compliance costs to private companies might.

Though the individual loss to each victim may not inspire political action, it can be quite considerable in the aggregate. In fact, even if increased cybersecurity measures added hundreds of millions of dollars in compliance costs for companies, it would still be dwarfed by the costs consumers bear when their personal information is exposed. These costs are often latent and hard to estimate, but the DOJ's recent report on identity theft concluded that 64.9% of the 17,576,200 victims of identity theft in 2014 suffered financial losses of greater than $1, with an average loss of $1343.[64] By these numbers, the cost to consumers in 2014 alone exceeded $15

2018-04-09/where-have-all-the-u-s-public-companies-gone (on file with the *Columbia Business Law Review*).

62 *QuickFacts*, U.S. CENSUS BUREAU (2012), https://www.census.gov/quickfacts/fact/table/US/SBO001212#SBO001212 [https://perma.cc/6NWA-HLU2].

63 *See About the FTC,* FED. TRADE COMMISSION, https://www.ftc.gov/about-ftc [https://perma.cc/Y4BT-N7YV].

64 HARRELL, *supra* note 26, at 6.

billion.[65] While not all identity theft is directly caused by data breaches, it is the motivation for most breaches.[66] With over 3.3 billion records compromised in the first half of 2018 alone,[67] if even a fraction of these resulted in financial loss from identity theft (at an average cost of $1343 per victim), the total cost to consumers would be astronomical.

Compounding their powerlessness, victims are politically disorganized strangers, while firms, especially large technology firms, are much more concentrated. This concentration allows companies to lobby much more effectively.[68] Put simply, there is no organized group of "Data Breach Victims" clamoring for reform. An enterprising private attorney may offer some organization by bringing a class action, duly incentivized by the potential contingency fee to be earned through aggregating claims. However, even if she overcomes the hurdles of winning such a case, the final damages may make for a very wealthy attorney but would barely effect the bottom line of a company like Facebook.

The FTC helps consumers cut through this Gordian knot. By representing all consumers, agency action helps even the playing field between individuals and corporations and acts as a concentrated conduit for their interests. Additionally, as an executive branch agency, it enjoys an extra degree of insulation from the interests that affect legislative decision-making.

Generally speaking, the FTC advances its mission of protecting consumers and competition by enforcing a variety of related laws. Before the 1970s, the FTC relied on its authority to bring actions against parties that violated the

65 *Id.* at 7.

66 *See Data Breaches Compromised 3.3 Billion Records in First Half of 2018*, GEMALTO (Oct. 23, 2018), https://www.gemalto.com/press/pages/data-breaches-compromised-3-3-billion-records-in-first-half-of-2018.aspx [https://perma.cc/XV2F-2LVV].

67 *Id.*

68 *See* TIM WU, THE CURSE OF BIGNESS 55 (2018).

Federal Trade Commission Act, the Clayton Act, or other consumer protection laws.[69]

In the early 1970s, however, the FTC began promulgating rules, and its authority to do so was upheld by the United States Court of Appeals for the District of Columbia Circuit.[70] Congress soon after passed two laws that delineated and circumscribed the FTC's rulemaking ability, the Magnuson-Moss Warranty—Federal Trade Commission Improvement Act of 1975[71] and the Federal Trade Commission Improvements Act of 1980.[72] These laws imposed additional procedures (collectively the "Magnuson-Moss Procedures") that complicated the FTC's rulemaking process and "go far beyond the relatively streamlined notice-and-comment procedures mandated in Section 553 of the [Administrative Procedure Act of 1946 ("APA")] to which most agencies are subject."[73] FTC rulemaking dramatically slowed following the passage of the Magnuson-Moss Procedures, but Congress has occasionally provided limited statutory authorization for the FTC to use the APA rulemaking procedures to issue specific rules.[74]

On three occasions, Congress has permitted the FTC to use APA rulemaking procedures to address prevalent online privacy and cybersecurity issues—children's privacy online, privacy of consumer financial data, and health data

[69] *See A Brief Overview of the Federal Trade Commission's Investigative and Law Enforcement Authority*, FED. TRADE COMMISSION (July 2008) [hereinafter *A Brief Overview*], https://www.ftc.gov/about-ftc/what-we-do/enforcement-authority [https://perma.cc/42YY-TGAY].

[70] *See* Nat'l Petroleum Refiners Ass'n v. FTC, 482 F.2d 672, 698 (D.C. Cir. 1973).

[71] *See* Magnuson-Moss Warranty—Federal Trade Commission Improvement Act, Pub. L. No. 93-637, § 202, 88 Stat. 2183, 1293 (1975) (codified as amended at 15 U.S.C. § 57a (2012)).

[72] *See* Federal Trade Commission Improvements Act of 1980, Pub. L. No. 96-252, §§ 7–12, 15, 21, 94 Stat. 374, 376–80, 388–90, 393–96 (codified as amended in scattered sections of 15 U.S.C).

[73] Jeffrey S. Lubbers, *It's Time to Remove the "Mossified" Procedures for FTC Rulemaking*, 83 GEO. WASH. L. REV. 1979, 1982 (2015).

[74] *See id.*

breaches.[75] However, without a broader Congressional mandate, rulemaking for all other categories of consumer data is subject to the Magnuson-Moss Procedures.[76] Though the FTC has not issued any rules concerning this large swath of data, it has brought enforcement actions under section 5 of the 1914 FTC Act against companies that have lost consumer data.[77] This Section briefly traces the development of the FTC's enforcement practices and then looks at the potential of rulemaking to complement the FTC's current efforts.

A. Adjudication

The FTC began policing corporate cybersecurity practices in 2002.[78] Though the 1914 FTC Act unsurprisingly makes no mention of cybersecurity, section 5 of the Act—prohibiting "unfair or deceptive acts or practices in or affecting commerce"[79]—was intended to be interpreted broadly, according to the statute's legislative history and subsequent Supreme Court decisions.[80] In the early 2000s, the FTC

[75] *See* Regulation of Unfair and Deceptive Acts and Practices in Connection with Collection and Use of Personal Information from and About Children on the Internet, 15 U.S.C. § 6502(b)(1) (2012); *see also* Rulemaking, 15 U.S.C. § 6804(a)(3) (2012); Temporary Breach Notification Requirement for Vendors of Personal Health Records and Other Non-HIPAA Covered Entities, 42 U.S.C. § 17937(g)(1) (2012).

[76] Requiring much more than simple notice and comment, the Magnuson-Moss Procedures mandate a much more laborious process. For a good overview, see Lubbers, *supra* note 73, at 1982–84.

[77] *See* FTC, PRIVACY & DATA SECURITY UPDATE: 2017, at 4 (2018), https://www.ftc.gov/system/files/documents/reports/privacy-data-security-update-2017-overview-commissions-enforcement-policy-initiatives-consumer/privacy_and_data_security_update_2017.pdf [https://perma.cc/9E98-SKX5].

[78] *See id.*; *see also* William R. Denny, *Cybersecurity as an Unfair Practice: FTC Enforcement Under Section 5 of the FTC Act*, BUS. L. TODAY, June 2016, at 2, 2, https://www.americanbar.org/content/dam/aba/publications/blt/2016/06/cyber-center-denny-201606.pdf [https://perma.cc/F2SP-RLLN].

[79] 15 U.S.C. § 45(a)(1) (2012).

[80] *See, e.g.*, FTC v. Sperry & Hutchinson Co., 405 U.S. 233, 239–40 (1972). *See generally* Neil W. Averitt, *The Meaning of "Unfair Methods of*

brought a number of actions against companies that failed to protect consumer data.[81] Early actions were based on the premise that, by making false representations about data security, companies were engaging in deceptive business practices.[82] Later actions were based on claims that companies' cybersecurity practices were "unfair."[83]

All actions until 2012 resulted in consent decrees,[84] whereby companies agreed to certain terms without admitting guilt.[85] Though some companies questioned the FTC's authority to regulate cybersecurity, they all settled to avoid drawn out litigation—and the resulting legal costs, potential public exposure, and reputational harm.[86] In 2012, however, Wyndham Worldwide Corp. ("Wyndham") challenged the FTC's authority in court. Following a series of hacks that exposed more than 600,000 records in Wyndham's possession and resulted in $10.6 million in fraudulent charges, the FTC brought a suit alleging unfair cybersecurity practices.[87] The

Competition" in Section 5 of the Federal Trade Commission Act, 21 B.C. L. REV. 227 (1980).

81 *See* FTC, *supra* note 77, at 4; *see also Cases Tagged with Data Security*, FED. TRADE COMMISSION, https://www.ftc.gov/enforcement/cases-proceedings/terms/249?page=2 [https://perma.cc/7LSD-6X33].

82 *See* Julie Brill, Commissioner, FTC, On the Front Lines: The FTC's Role in Data Security, Keynote Address Before the Center for Strategic and International Studies: "Stepping into the Fray: The Role of Independent Agencies in Cybersecurity" 3 (Sept. 17, 2014), (available at https://www.ftc.gov/system/files/documents/public_statements/582841/140917csisspeech.pdf [https://perma.cc/Y5JE-RRBA]) ("The FTC's data security enforcement actions initially focused on deception.").

83 *See id.* at 4.

84 M. Sean Royall et al., *The Third Circuit Upholds the U.S. Federal Trade Commission's Authority to Regulate Cybersecurity*, GIBSON DUNN (Aug. 27, 2015), https://www.gibsondunn.com/the-third-circuit-upholds-the-u-s-federal-trade-commissions-authority-to-regulate-cybersecurity/ [https://perma.cc/Z8EJ-3ZXM].

85 Consent decrees are settlements with the FTC and do not include any findings made by a court. *See Consent Decree*, WEST'S ENCYCLOPEDIA OF AMERICAN LAW (2d ed. 2004).

86 Denny, *supra* note 78.

87 FTC v. Wyndham Worldwide Corp., 799 F.3d 236, 242 (3d Cir. 2015); *see also* Denny, *supra* note 78.

district court denied Wyndham's motion to dismiss, but Wyndham appealed the question of whether the "unfairness" prong of section 5 applied to cybersecurity.[88] The Third Circuit held that it did,[89] judicially affirming the FTC's authority.

As the FTC worked its way to a final settlement with Wyndham, another company, LabMD, Inc. ("LabMD"), commenced its own challenge to another FTC attempt at cybersecurity enforcement. LabMD, a clinical testing laboratory, stored personal information for nearly one million consumers.[90] In 2013, the FTC filed an Administrative Complaint identifying two "security incidents" and charged LabMD with "failure to employ reasonable and appropriate measures to prevent unauthorized access to personal information, including dates of birth, [Social Security numbers], medical test codes, and health information" that "caused, or is likely to cause, substantial injury to consumers that is not offset by countervailing benefits to consumers or competition and is not reasonably avoidable by consumers."[91] The FTC alleged that these failures amounted to unfair business practices in violation of section 5 of the FTC Act.[92]

An administrative law judge ("ALJ") dismissed the complaint, finding that the FTC failed to meet its burden of proving the alleged conduct caused or is likely to cause substantial injury to consumers.[93] The judge stated, "[a]t best, Complaint Counsel has proven the 'possibility' of harm, but not any 'probability' or likelihood of harm" and that "[f]undamental fairness dictates that demonstrating actual or likely substantial consumer injury under Section 5(n) requires proof of more than the hypothetical or theoretical harm that has been submitted by the government in this case."[94]

88 *Wyndham*, 799 F.3d at 242.

89 *Id.* at 249.

90 *See* Complaint at *2, *In re* LabMD, Inc., F.T.C. No. 9357, 2013 WL 5232775 (Aug. 29, 2013).

91 *Id.* at *4–5.

92 *Id.* at *5.

93 *See* Initial Decision at *13, *In re* LabMD, Inc., F.T.C. No. 9357, 2015 WL 7575033 (Nov. 13, 2015).

94 *Id.* at *14.

The FTC appealed this decision to its own commissioners, who unsurprisingly reversed and ruled in favor of the agency.[95] The Commission vacated the ALJ's decision and ordered LabMD to install a data-security program that met the FTC's reasonableness standard.[96] Up to this point, the FTC's strategy of promoting security standards through enforcement actions appeared workable. However, the most recent development in the case has left the future efficacy of the FTC's enforcement through adjudication in question.

Following the Commission's final order, LabMD sought judicial review of the order in the Eleventh Circuit. The Eleventh Circuit vacated the order, agreeing with LabMD's argument that it was unenforceable.[97] Notably, the court did not decide whether LabMD's conduct constituted an unfair business practice, but merely assumed arguendo that it did.[98] Even with this assumption, the Court held the order—"founded upon LabMD's general negligent failure to act"—was unenforceable as it did not elucidate a specific act for LabMD to cease and desist.[99] The Court reasoned that "the cease and desist order contains no prohibitions. It does not instruct LabMD to stop committing a specific act or practice. Rather, it commands LabMD to overhaul and replace its data-security program to meet an indeterminable standard of reasonableness. This command is unenforceable."[100]

This decision carries wide-ranging implications for the regulation of consumer data—potentially impacting the FTC's future enforcement strategy. As mentioned, aside from the *Wyndham* and *LabMD* cases, the FTC has resolved dozens of

95 *See* Opinion of the Commission, at *1, *In re* LabMD, Inc., F.T.C. No. 9357, 2016 WL 4128215 (Jul. 28, 2016) ("[T]he Commission has concluded that LabMD's data security practices were unreasonable and constitute an unfair act or practice that violates Section 5 of the Federal Trade Commission Act.").

96 *Id.* at *1–2.

97 *See* LabMD, Inc. v. FTC, 894 F.3d 1221, 1224 (11th Cir. 2018).

98 *See id.* at 1231.

99 *Id.*

100 *Id.* at 1236.

data privacy issues with consent decrees.[101] The Commission advertises these as providing notice to the private sector of compliance expectations.[102] While the Commission appealed the ALJ's dismissal, it argued, "the FTC has been consistent and clear about how it enforces Section 5 of the FTC Act against companies for their business practices related to the security of consumer data and, as a result, Respondent has received fair notice."[103] The Eleventh Circuit's decision in *LabMD*, finding the FTC's order to be unenforceable, calls into question the validity of the Commission's past enforcement actions—many of which employed language identical to the vacated LabMD order.[104] It also provides the FTC with reason to reevaluate its enforcement philosophy and seek a less disputable method of giving notice to private companies. This opens the door for promulgating rules, as discussed below.

The Eleventh Circuit's decision may also increase pressure on Congress to enact federal legislation establishing a uniform national regime, or at least pass a mandate giving the FTC specific cybersecurity enforcement power. The decision also leaves several questions unresolved, including whether a data breach constitutes an unfair act or practice and whether it results in actionable harm under the FTC Act. This ambiguity opens future FTC enforcement to additional challenges. A Congressional mandate would bypass these issues by establishing independent authorization and could clearly define lost data as an injury.

101 *See* FTC, *supra* note 77.

102 *See* FED. TRADE COMM'N, START WITH SECURITY: A GUIDE FOR BUSINESS 1 (2015), https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf [https://perma.cc/6KPX-QAJW] ("There's another source of information about keeping sensitive data secure: the lessons learned from the more than 50 law enforcement actions the FTC has announced so far.").

103 *See* Complaint Counsel's Response in Opposition to Respondent's Motion to Dismiss Complaint with Prejudice and to Stay Administrative Proceedings at *20, *In re* LabMD, Inc., F.T.C. No. 9357, 2013 WL 6327988 (Nov. 22, 2013).

104 *See, e.g.*, *In re* James B. Nutter & Co. F.T.C. No. C-4258, 2009 WL 1818012 (June 12, 2009) (decision and order).

B. Rulemaking

In addition to bringing enforcement actions, the FTC has the authority to promulgate rules consistent with its mission.[105] The FTC has used its rulemaking authority infrequently, however, since the passage of the Magnuson-Moss Procedures.[106] Still, despite the obstacles the FTC faces in promulgating rules, the current state of cybersecurity regulation may require the agency to dust off this dormant tool.

The *Wyndham* and *LabMD* cases demonstrate some of the factors that hamper the FTC's ability to effectively regulate through adjudication. Unlike in the field of children's privacy, the FTC lacks the statutory authority to impose civil penalties for consumer privacy issues.[107] As a result, first-time offenders often receive what Commissioner Rohit Chopra called a mere "slap on the wrist,"[108] a characterization echoed by many observers.[109] While Wyndham was technically a

105 "[T]he Commission may use trade regulation rules to remedy unfair or deceptive practices that occur on an industry-wide basis." *A Brief Overview*, *supra* note 69.

106 *See* Lubbers, *supra* note 73, at 1989.

107 *See* Cat Zakrzewski, *The Technology 202: Is the FTC Powerful Enough to Be an Effective Privacy Cop? New Report Raises Questions*, WASH. POST (Feb. 14, 2019), https://www.washingtonpost.com/news/powerpost/paloma/the-technology-202/2019/02/14/the-technology-202-is-the-ftc-powerful-enough-to-be-an-effective-privacy-cop-new-report-raises-questions/5c6462e51b326b71858c6b79/?utm_term=.c6c1584d329f [https://perma.cc/4DH2-XESP].

108 *Opening Statement of Commissioner Rohit Chopra: Hearing on Oversight of the Federal Trade Commission Before the Subcomm. on Consumer Prot., Product Safety, Ins., & Data Sec. of the S. Comm. on Commerce, Sci., & Transp.*, 115th Cong. 1 (2018) (statement of Rohit Chopra, Comm'r, Fed. Trade Comm'n), https://www.ftc.gov/system/files/documents/public_statements/1423961/chopra_oral_remarks_for_november_2018_senate_commerce_hearing.pdf [https://perma.cc/2QLB-N7NW].

109 *See* Brady Dale, *FTC Slaps the Wrist of Tax Prep Service After 8,800 Customers' Data Breached*, OBSERVER (Aug. 30, 2017), https://observer.com/2017/08/ftc-taxslayer/ [https://perma.cc/MGF5-WL4W]; Allison Grande, *LabMD Gets Slap On Wrist In FTC Data Security Fight*, LAW360 (Mar. 13, 2014), https://www.law360.com/articles/518274 (on

"first-time offender"—having received no previous settlement with the FTC, the Third Circuit held that the company had fair notice,[110] noting that the company had been hacked three times and, "after the second attack, it should have been painfully clear to Wyndham that a court could find its conduct failed the cost-benefit analysis."[111] However, waiting for multiple successive hacks before imposing penalties is a patently inefficient regulatory strategy. Alternatively, the FTC can seek civil penalties against a company that has violated a previously issued injunction or consent decree.[112] This solution is also imperfect—it effectively requires the FTC to bring two actions against any firm in order to penalize it. The infeasibility of this approach is compounded by the fact that even some of the FTC's injunctions have been found unenforceable.[113]

Despite this uphill battle, the FTC has continued to use its authority to issue consent decrees,[114] which at least allows enforcement of civil penalties against second-time violators. For instance, some Senators believe Google's recent data

file with the *Columbia Business Law Review*); David Kravets, *FTC Slaps Facebook's Hand Over Privacy Deception*, WIRED (Nov. 29, 2011), https://www.wired.com/2011/11/ftc-slaps-facebook-privacy/ [https://perma.cc/VT7X-Z4J4]; David Kravets, *FTC Slaps Google's Wrist in Search, Patent Probe*, WIRED (Jan. 3, 2013), https://www.wired.com/2013/01/ftc-google-patent-search-probe/ [https://perma.cc/PC8L-L84G]; Linda McGlasson, *Reaction to TJX Settlement: "A Very Light Slap on the Wrist*,*"* BANK INFO SECURITY (Mar. 28, 2008), https://www.bankinfosecurity.com/reaction-to-tjx-settlement-a-very-light-slap-on-wrist-a-793 [https://perma.cc/E6FE-GX3H].

110 FTC v. Wyndham Worldwide Corp., 799 F.3d 236, 255 (3d Cir. 2015).

111 *Id.* at 256.

112 *See The Enforcers*, FED. TRADE COMMISSION, https://www.ftc.gov/tips-advice/competition-guidance/guide-antitrust-laws/enforcers [https://perma.cc/9772-F5Q9].

113 *See* LabMD, Inc. v. FTC, 894 F.3d 1221, 1224 (11th Cir. 2018).

114 *See, e.g.*, Press Release, Fed. Trade Comm'n, Uber Agrees to Expanded Settlement with FTC Related to Privacy, Security Claims (Apr. 12, 2018), https://www.ftc.gov/news-events/press-releases/2018/04/uber-agrees-expanded-settlement-ftc-related-privacy-security [https://perma.cc/729S-GBQU].

breach violates its 2011 consent decree with the FTC.[115] Because the previous consent decree constituted notice, the FTC may now seek civil penalties against Google if the agency finds a violation. However, the recent LabMD decision brings the efficacy of such consent decrees into question.

If the FTC's capacity to promulgate rules offers a potential solution to the notice problem, why has it not done so? A look at the history of FTC rulemaking offers some insight.

1. History of the FTC's Rulemaking Process

For most of the FTC's history, it relied solely on adjudicative enforcement. In 1973, however, the agency's authority to promulgate rules survived its first judicial challenge.[116] After the FTC's rulemaking authority was upheld in the courts, Congress quickly grew tired of what it viewed as "the second most powerful legislature in Washington."[117] As the FTC zealously pursued initiatives in what is widely considered the agency's activist era,[118] Congress sought to circumscribe the Commission's rulemaking authority.[119] To do so, Congress passed the Magnuson-Moss Act and Federal Trade Commission Improvements Act of 1980.[120] These laws made it significantly more difficult for the FTC to promulgate rules by mandating additional rulemaking procedures—many of which afford

115 *Two Democrats Say Google+ Data Exposure May Violate FTC Consent Decree*, REUTERS (Oct. 24, 2018), https://www.reuters.com/article/google-congress/two-democrats-say-google-data-exposure-may-violate-ftc-consent-decree-idUSL2N1X40SF [https://perma.cc/2JX9-V95Z].

116 *See* Nat'l Petroleum Refiners Ass'n v. FTC., 482 F.2d 672, 698 (D.C. Cir. 1973).

117 *Financial Services and Products: The Role of the Federal Trade Commission in Protecting Customers—Part II: Hearing Before the Subcomm. on Consumer Prot., Product Safety, & Ins. of the S. Comm. on Commerce, Sci., & Transp.*, 111th Cong. 63 (2011) (testimony of Timothy J. Muris, Foundation Professor, George Mason University School of Law, and Of Counsel, O'Melveny & Myers LLP).

118 *See* MICHAEL PERTSCHUK, REVOLT AGAINST REGULATION: THE RISE AND PAUSE OF THE CONSUMER MOVEMENT 73 (1982).

119 *See id.*

120 *See supra* Part III.

opponents of proposed regulations the opportunity to significantly impede the efforts.[121]

The alternative rulemaking regime is the Administrative Procedure Act ("APA"), which exclusively governed FTC rulemaking before the enactment of Magnuson-Moss and the FTC Improvement Act of 1980 and governs many of the rulemaking procedures used by other agencies.[122] The APA provides for a considerably more streamlined notice-and-comment process.[123] Occasionally, Congress has passed legislation allowing the FTC to utilize the APA procedures in select circumstances.[124] Recently, the FTC requested authority to use the APA process in promulgating cybersecurity rules.[125]

2. Significance of Using APA Rulemaking Process

No new rules have been initiated under the Magnuson-Moss Procedures since they were further complicated by the FTC Improvements Act in 1980.[126] The FTC has followed the

[121] Such procedures include, in many commonly-applicable circumstances, mandatory oral hearings upon request and a requirement that interested parties be granted opportunities for cross-examination. *See generally* 15 U.S.C. § 57a (2012).

[122] *See generally* 5 U.S.C. § 553 (2012).

[123] *See generally id.*; *see also* Lubbers, *supra* note 73, at 1982.

[124] *See, e.g.*, 15 U.S.C. §§ 6501–6506 (2012).

[125] *See Prepared Statement of the Federal Trade Commission: Oversight of the Federal Trade Commission Before the Subcomm. on Consumer Prot., Product Safety, Ins., & Data Sec. of the S. Comm. on Commerce, Sci., & Transp.*, 115th Cong. 8 (2018) [hereinafter *Oversight of the FTC*], https://www.commerce.senate.gov/public/_cache/files/b899ff99-268a-42bb-8e85-8614c8b89d77/6ED6F7BF777A99734587437B1B6DB6E0.11-27-2018ftc-testimony.pdf [https://perma.cc/K6CJ-8P3C].

[126] *See* Lubbers, *supra* note 73, at 1989; *see also* Jon Leibowitz, Chairman, FTC, Remarks at the Association of National Advertisers Advertising Law and Public Policy Conference (Mar. 18, 2010) (available at https://www.ftc.gov/sites/default/files/documents/public_statements/association-national-advertisers-advertising-law-and-public-policy-conference-prepared-delivery/100318nationaladvertisers.pdf [https://perma.cc/MC3E-3PRH]) ("The requirements to promulgate a rule under [the Magnuson-Moss Act] are so onerous that the agency has not proposed a new [Magnuson-Moss Act] rule in 32 years. Thirty-two. For instance, under [the

procedures to amend previously promulgated rules, but it took the agency an average of 5.26 years to complete these amendments.[127] For comparison, in the limited circumstances where Congress asked the FTC to make rules according to APA procedures, it took an average of 287.3 days—less than one year.[128] It is particularly illustrative to consider the FTC's promulgation of another privacy rule, the Financial Privacy Rule. When Congress passed the Gramm-Leach-Bliley Act—which gives federal banking agencies authority to regulate financial data[129]—it asked the FTC to make a rule under the APA procedures.[130] The FTC issued its notice of proposed rulemaking on March 1, 2000, and after receiving 640 comments, issued its final rule on May 24, 2000—84 days later.[131]

While the Magnuson-Moss Procedures have effectively frozen the FTC's ability to promulgate rules, the APA offers a method for the FTC to develop rules benefiting consumers in the same way other agencies make their cybersecurity regulations. Congress need not grant the FTC broad legislative authority; it simply should allow the FTC to invoke APA procedures in this limited rulemaking context.

IV. FOR BEST RESULTS, USE THE WHOLE TOOLKIT

Implementing a simple solution to protect consumer data is far from easy, but using its various tools, the FTC is the best-positioned federal agency to provide a path forward. While there have been increasing calls for federal intervention, specific standards promulgated by Congress are

Magnuson-Moss Act], if any member of the public requests it, the agency has to hold a hearing where interested persons have the right to examine, rebut, and cross-examine witnesses.").

127 Lubbers, *supra* note 73, at 1991.

128 *Id.* at 1995.

129 *See* 15 U.S.C. § 6801 (2012).

130 *See id.* § 6804(a)(3).

131 *See* Lubbers, *supra* note 73, at 1993–94.

at risk of inadequately protecting consumers.[132] Amidst these calls for legislation, rather than allowing the companies subject to the regulation to dictate its terms, Congress should look to the consumer protection experts at the FTC and afford them the ability to propose cybersecurity rules and receive comments. The FTC is an agency specifically designed to protect the interests of consumers who may otherwise lack the organizational capacity or financial incentive to do so alone. It also enjoys relative insulation from political pressure.[133]

While the FTC may be the ideal vehicle for promulgating regulations that sufficiently protect consumers, it is hamstrung by procedural barriers.[134] Given the FTC's broad scope of authority, Congress may have had good reason to restrict its rulemaking ability. But by doing so, Congress has left consumers' data vulnerable. Congress can lift these rulemaking restrictions for the limited purpose of allowing the FTC to address data security. It has done so in the past, allowing the Commission to utilize APA rulemaking mechanisms "for discrete topics such as children's privacy, financial data security, and certain provisions of credit reporting."[135] Under this lightened procedural burden, the FTC would likely be able to establish a regulatory framework in a matter of months. Moreover, if such a congressional rulemaking mandate preempted state laws, it could eliminate the compliance headache for companies operating under inconsistent state laws without undercutting the progress made by the states to protect consumer data. Additionally, such a congressional mandate could formalize definitions of

[132] Large companies are already involved in designing the regulations to which they may be subject. *See* David Shepardson, *Trump Administration Working on Consumer Data Privacy Policy*, REUTERS (July 27, 2018), https://www.reuters.com/article/us-usa-internet-privacy/trump-administration-working-on-consumer-data-privacy-policy-idUSKBN1KH2MK [https://perma.cc/SE6B-EM8T].

[133] *See* Paul R. Verkuil, *The Purposes and Limits of Independent Agencies*, 1988 DUKE L.J. 257, 259–60 (1988) (noting that independent agencies are "designed to isolate those decisionmakers from politics").

[134] *See supra* Section III.B.2.

[135] *See Oversight of the FTC*, *supra* note 125, at 8 n.20.

harm and thereby make adjudicative enforcement easier for the FTC.

Well-designed rules could resolve many pertinent issues in cybersecurity. They could close the gap in federal regulation of data security by extending regulations to all institutions, not just discrete sectors of the economy. They can also promote data breach prevention rather than self-flagellating disclosures.[136] Establishing these rules would allow the FTC to transform the advisory information within its online best practice guides[137] and various consent decrees into legally enforceable regulations. The Commission can grow the teeth it needs.

V. CONCLUSION

The staggering data breach statistics and costs of identity theft highlight the gaps in federal cybersecurity regulation and the need for improvement. Many other countries have responded and so have states—even if their efforts have created a growing thicket of compliance standards. The FTC is doing what it can through adjudication, but employing its rarely used rulemaking authority can increase its regulatory efficacy. Consumers need protection, and the consumer protection agency has the tools to provide it.

136 *See* O'Connor, *supra* note 10.

137 *See, e.g.*, FED. TRADE COMM'N, *supra* note 102.