EMORY | LAW

Emory Law Journal

Volume 69 | Issue 4 Article 4

2020

Resurrecting Magnuson-Moss Rulemaking: The FTC at a Data Security Crossroads

Ian M. Davis

RESURRECTING MAGNUSON-MOSS RULEMAKING: THE FTC AT A DATA SECURITY CROSSROADS

ABSTRACT

Welcome to the digital age, where consumer data is more valuable than gold. In this era of information, companies treat personal data as a prized commodity, leveraging its potential to boost business and engage an ever-growing number of customers. Yet when companies fail to protect the sensitive data that they hold, consumers are left with few avenues to obtain redress for the harms they may have suffered. In an effort to protect consumers, the Federal Trade Commission (FTC) has been policing inadequate data security practices since the early 2000s. Using its broad authority under Section 5 of the Federal Trade Commission Act, the FTC routinely brings enforcement actions against companies that have sustained data breaches, yet could have implemented reasonable security measures to prevent them. In the vast majority of proceedings, the violating entity chooses to settle with the FTC rather than incur the various costs associated with litigation. The orders that accompany the conclusion of every enforcement proceeding typically require the violator to enact a comprehensive data security overhaul.

In 2018, such an FTC order was vacated by the U.S. Court of Appeals for the Eleventh Circuit. On the heels of this decision, it is apparent that the FTC must recalibrate its approach to enforcing unlawful data security practices. This Comment contends that the Commission should draw on its substantial experience with data protection and promulgate a rule that transparently specifies the standard by which data security is to be regulated. Although the FTC's decision to abstain from using its Magnuson-Moss rulemaking authority may have been prudent in the early days of its foray into data security, times have changed. Embracing the heightened public participation interwoven throughout the hybrid rulemaking process, the FTC is fully capable of delineating a data security standard in a reasonable amount of time. And once the rule-based standard is in place, the FTC can reap the benefits of a framework that provides the regulated community with enhanced guidance and the consumer public with greater protection from preventable data harms.

INTRODUCTION 783
I. THE U.S. ADMINISTRATIVE APPROACH TO DATA SECURITY 787
A. *The Federal Trade Commission: America's Primary Data Regulator* 789
1. *A Brief Survey of the FTC's Consumer Protection Authority* 790
2. *Section 5: Unfair or Deceptive Acts or Practices* 792
3. *Enforcing Violations of Section 5* 795
B. *The FTC's Rulemaking Authority* 797
1. *Nonlegislative Rules* 798
2. *Legislative Rules: The Magnuson-Moss Act & Trade Regulation Rules* 800
II. RECENT FTC DEVELOPMENTS IN DATA SECURITY 803
A. *LabMD at the FTC: Demystifying Consumer Data Breach Harms* 804
B. *LabMD at the Eleventh Circuit: The Virtues of Specificity* 808
III. THE PATH FORWARD: A RETURN TO MAGNUSON-MOSS RULEMAKING 811
A. *Why the FTC Should Promulgate a Magnuson-Moss Data Security Rule* 813
B. *Anticipating Judicial Review: How the FTC Can Formulate a Durable Data Security Rule* 821
1. *Expeditiously Sticking to Procedure* 821
2. *Defining Unfair Data Security Acts with Specificity* 825
3. *Preemption* 829
CONCLUSION 831

INTRODUCTION

On September 7, 2017, the credit-monitoring service Equifax announced that it had sustained a data breach[1] of alarming proportions.[2] As the dust settled, it became apparent that the personally identifiable information[3] of nearly 147 million U.S. consumers had been compromised.[4] The unprecedented attack resulted in the loss of 146.6 million consumer names and dates of birth, 145.5 million Social Security numbers, 99 million addresses, 20.3 million phone numbers, 17.6 million driver's license numbers, 209,000 credit card numbers, and 97,500 taxpayer identification numbers.[5]

Although Equifax was the victim of a concerted criminal act, the company was publicly criticized for its allegedly insufficient security protocols and "ham-fisted" response to the breach.[6] Consumers were understandably mortified at the extent of the breach and the knowledge that their private information was in the

---

[1] A data breach is generally defined as the "unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of sensitive personal information." TEX. BUS. & COM. CODE ANN. § 521.053 (West 2018). All fifty states have data breach notification laws (DBNLs) that define the term, with some subtle differences. *Compare, e.g.*, WASH. REV. CODE § 19.255.010(4) (2018) ("unauthorized acquisition of data that compromises the security, confidentiality, or integrity of personal information maintained by the person or business"), *with* NEV. REV. STAT. § 603A.020 (2018) ("unauthorized acquisition of computerized data that materially compromises the security, confidentiality or integrity of personal information maintained by the data collector").

[2] *See Equifax Announces Cybersecurity Incident Involving Consumer Information*, EQUIFAX (Sept. 7, 2017), https://investor.equifax.com/news-and-events/news/2017/09-07-2017-213000628.

[3] Although no uniform definition of personally identifiable information (PII) exists, the Department of Commerce's National Institute of Standards and Technology has defined it as "any information that can be used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother's maiden name, or biometric records; and any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information." NAT'L INST. OF STANDARDS AND TECH., SPECIAL PUB. 800-122, GUIDE TO PROTECTING THE CONFIDENTIALITY OF PERSONALLY IDENTIFIABLE INFORMATION 2-1 (2010).

[4] *See Equifax, Statement for the Record Regarding the Extent of the Cybersecurity Incident Announced on September 7, 2017*, SEC. & EXCHANGE COMMISSION (May 7, 2018), https:/www.sec.gov/Archives/edgar/data/33185/000119312518154706/d583804dex991.htm.

[5] *See id.*

[6] Hamza Shaban, *'This Is a Travesty:' Lawmakers Grill Former Equifax Chief Executive on Breach Response*, WASH. POST (Oct. 3, 2017), https://www.washingtonpost.com/news/the-switch/wp/2017/10/02/what-to-expect-from-equifaxs-back-to-back-hearings-on-capitol-hill-this-week/?utm_term=.095ef231eca0 (reporting that Representative Greg Walden of Oregon, the Chairman of the House Energy and Commerce Committee, described Equifax's post-breach response as "ham-fisted"); *see* Farhad Manjoo, *Seriously, Equifax? This Is a Breach No One Should Get Away With*, N.Y. TIMES (Sept. 8, 2017), https://www.nytimes.com/2017/09/08/technology/seriously-equifax-why-the-credit-agencys-breach-means-regulation-is-needed.html.

hands of nefarious hackers.[7] Yet, as lawsuits[8] and investigations[9] commenced, the post-Equifax legal narrative has paid little attention to the plight of consumers.

But how can a consumer's post-breach harm be properly characterized? Under contemporary legal mechanisms, this task is notoriously difficult.[10] To demonstrate, imagine that Bernard, an ordinary consumer, was notified that his personal data was implicated in the Equifax data breach.[11] Hackers are now capable of exploiting Bernard's Social Security number and credit card details to commit identity theft, financial fraud, or any number of other illicit acts.[12] Understandably, Bernard is anxious at the prospect of these potential outcomes. Accordingly, he takes a number of prophylactic steps to ensure that his data is not misused. He cancels and replaces his credit cards and checks, updates his new financial information with digital vendors, freezes his credit, and purchases identity theft protection. Through all this, Bernard has not yet suffered an actual injury. Instead, Bernard now faces an increased risk of future harm.[13] Although Bernard's increased risk of harm is difficult to legally classify, it is not without merit. In the most basic of terms, Equifax's inadequate data security has left Bernard in a worse position than before.

Any business that hopes to compete in the modern marketplace must contend with the various risks and rewards that accompany the use of consumer data.[14]

---

[7] *See, e.g.*, Niraj Chokshi, *How a Few People Took Equifax to Small Claims Court over Its Data Breach and Won*, N.Y. TIMES (June 20, 2018), https://www.nytimes.com/2018/06/20/business/equifax-hack-small-claims-court.html (describing consumers' "frustration and sense of helplessness after the [Equifax] breach").

[8] *See, e.g.*, *In re* Equifax, Inc., Customer Data Sec. Breach Litig., 289 F. Supp. 3d 1322 (J.P.M.L. 2017).

[9] *See, e.g.*, Tara Siegel Bernard, *Prosecutors Open Criminal Investigation into Equifax Breach*, N.Y. TIMES (Sept. 18, 2017), https://www.nytimes.com/2017/09/18/business/equifax-breach-federal-investigation.html; David McLaughlin & Todd Shields, *FTC Opens Investigation into Equifax Breach*, BLOOMBERG (Sept. 14, 2017, 6:20 PM), https://www.bloomberg.com/news/articles/2017-09-14/equifax-scrutiny-widens-as-ftc-opens-investigation-into-breach.

[10] *See, e.g.*, Woodrow Hartzog & Daniel J. Solove, *The Scope and Potential of FTC Data Protection*, 83 GEO. WASH. L. REV. 2230, 2233 (2015) ("[T]he law has struggled to recognize privacy violations and data security breaches as harms."); Daniel J. Solove & Danielle Keats Citron, *Risk and Anxiety: A Theory of Data-Breach Harms*, 96 TEX. L. REV. 737, 739 (2018) ("The concept of harm stemming from a data breach has confounded … courts.").

[11] EQUIFAX, *supra* note 2.

[12] *See generally* Kimberly Kiefer Peretti, *The Underground World of Online Identity Theft: An Overview*, *in* DATA BREACH AND ENCRYPTION HANDBOOK 49, 49–53 (Lucy Thomson ed., 2011) (providing an overview of the ways in which a hacker can exploit consumer data).

[13] *See* Solove & Citron, *supra* note 10, at 745 ("Victims of data breaches have an increased risk of identity theft, fraud, and reputational damage.").

[14] *See, e.g.*, Asuncion Esteve, *The Business of Personal Data: Google, Facebook, and Privacy Issues in the EU and the USA*, 7 INT'L DATA PRIVACY L. 36, 37 (2017) (discussing the corporate monetization of users' personal data).

Such data can be a powerful analytic tool, providing profit-seeking entities with valuable insight into the expected habits and preferences of consumers.[15] This insight can be leveraged in a variety of ways.[16] For example, companies routinely use consumer data to launch targeted advertising campaigns, conduct market analysis, develop their latest products and services, and individualize consumer experiences.[17] And unbeknownst to many consumers, there is even an entire industry of companies that broker personal data to other firms.[18]

When a company does sustain a data breach, the consequences can be immense.[19] Hacked companies typically experience public naming-and-shaming,[20] with potentially harmful public relations and financial consequences.[21] They must fulfill the many obligations imposed by state data breach notification laws[22] and may be brought to court by a class of consumers whose data was implicated in the breach.[23] Finally, hacked companies may be

---

[15] *See* FED. TRADE COMM'N, BIG DATA: A TOOL FOR INCLUSION OR EXCLUSION? UNDERSTANDING THE ISSUES 1 (2016) ("[W]hen consumers engage digitally … companies collect information about their choices, experiences, and individual choices.").

[16] *See, e.g.*, *id.* at 4–5 (discussing the use of data analytics in the digital marketplace).

[17] *See, e.g.*, *id.* at 1 ("The analysis of … consumer information is often valuable to companies and to consumers, as it provides insights into market-wide tastes and emerging trends, which can guide the development of new products and services. It is also valuable to predict the preferences of specific individuals, help tailor services, and guide individualized marketing of products and services."); *Privacy Policy, Why Google Collects Data*, GOOGLE PRIVACY & TERMS, https://policies.google.com/privacy?hl=en&gl=ZZ#whycollect (last visited Oct. 11, 2018) ("We use the information we collect to customize our services to you, including … personalized content, and … personalized ads.").

[18] *See generally* Max N. Helveston, *Consumer Protection in the Age of Big Data*, 93 WASH. U. L. REV. 859, 868 (2016) ("[T]he public is largely unaware of the of the rapid growth of the data industry and the extent to which individuals' personal information has become a commodity that is transferred among private and public entities.").

[19] *See, e.g.*, PONEMON INST., 2018 COST OF DATA BREACH STUDY: IMPACT OF BUSINESS CONTINUITY MANAGEMENT 11 (2018) (finding that the average total cost of a data breach is $3.86 million).

[20] *See, e.g.*, Brian Fung, *Actually, Every Single Yahoo Account Got Hacked in 2013*, WASH. POST (Oct. 3, 2017), https://www.washingtonpost.com/news/the-switch/wp/2017/10/03/yahoos-2013-data-breach-affected-all-3-billion-accounts-tripling-its-previous-estimate/?noredirect=on&utm_term=.ae0d726c5c07; Mike Isaac & Sheera Frenkel, *Facebook Security Breach Exposes Accounts of 50 Million Users*, N.Y. TIMES (Sept. 28, 2018), https://www.nytimes.com/2018/09/28/technology/facebook-hack-data-breach.html.

[21] *See, e.g.*, PONEMON INST., *supra* note 19, at 5; Kate Palmer & Cara McGoogan, *TalkTalk Loses 101,000 Customers After Hack*, TELEGRAPH (Feb. 2, 2016 10:15 AM), https://www.telegraph.co.uk/technology/2016/02/02/talktalk-loses-101000-customers-after-hack/; *News Release*, EQUIFAX (Apr. 25, 2018), https://www.sec.gov/Archives/edgar/data/33185/000003318518000017/exhibit99120180331.htm ("Since the announcement of the cybersecurity incident in September 2017, we have incurred a total of $242.7 million of expenses related to the incident and incremental IT and data security costs.").

[22] *See, e.g.*, CAL. CIV. CODE §§ 1798.29, 1798.82 (West 2018); N.Y. GEN. BUS. LAW § 899-aa (West 2018).

[23] *See, e.g.*, *In re* Arby's Rest. Grp. Inc. Litig., 317 F. Supp. 3d 1222 (N.D. Ga. 2018).

subject to Federal Trade Commission investigations, which can result in enforcement proceedings, remedial measures, and even monetary penalties.[24]

Yet to what extent do these various legal mechanisms protect the American consumer? In the digital age, consumers have little choice but to entrust profit-seeking companies with their personal information.[25] And when such information is compromised in a breach, affected individuals have few viable means of obtaining direct redress.[26]

As the leading federal regulatory body in the realm of data security, the Federal Trade Commission (the "FTC" or the "Commission") has shown that it is uniquely situated to protect consumers.[27] And to date, its prominence has yielded laudable results.[28] However, the FTC can and should do more to protect consumers from inadequate data security practices.

Despite its congressional grant of rulemaking authority, the FTC has declined to promulgate a regulatory rule identifying the boundaries of unlawful data security.[29] This Comment contends that after nearly twenty years of regulating data security through cases brought and settled under Section 5(a) of the Federal Trade Commission Act of 1914, the FTC would be well-advised to chart a new course. While congressional action, either through the expansion of FTC authority or the enactment of comprehensive data security legislation, presents an ambitious way to wipe the data security regulatory slate clean, the FTC cannot simply wait around while hackers continue to exploit digital vulnerabilities. The FTC can and should operate sensibly, using the means currently available to it, in order to codify the most basic data security responsibilities required of corporate America. In this way, the FTC can better protect consumers in the digital world.

---

[24] *See, e.g.*, Complaint for Injunctive and Other Equitable Relief, F.T.C. v. Accusearch Inc., F.T.C. v. Accusearch, Inc., 2007 WL 4356786, at *1 (D. Wyo. Sept. 28, 2007) (No. 06-CV-105-D), *aff'd*, 570 F.3d 1187 (10th Cir. 2009); Consent Order at 5, Facebook, Inc., No. C-4365 (F.T.C. Nov. 29, 2011).

[25] *See, e.g.*, Julia Alpert Gladstone, *Data Mines and Battlefields: Looking at Financial Aggregators To Understand the Legal Boundaries and Ownership Rights in the Use of Personal Data*, 19 J. MARSHALL J. COMPUTER & INFO. L. 313, 329 (2001) (noting that companies' "use of customer databases has become a critical strategy to successful business").

[26] *See, e.g.*, Joel R. Reidenberg, *Privacy Wrongs in Search of Remedies*, 54 HASTINGS L.J. 877, 877 (2003) (noting that under the U.S. legal framework, "privacy wrongs are currently in search of remedies").

[27] *See, e.g*, Daniel J. Solove & Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, 114 COLUM. L. REV. 583, 600 (2014) (noting that "many privacy lawyers and companies view the FTC as a formidable enforcement power, and they closely scrutinize FTC actions in order to guide their decisions").

[28] *See, e.g.*, Hartzog & Solove, *supra* note 10, at 2269–71 (arguing that the FTC is the "a key linchpin in the U.S. data protection regulatory regime").

[29] *See* 15 U.S.C. § 57a(a) (2012) ("Authority of the Commission to Prescribe Rules").

This Comment will unfold in three parts. Part I begins by describing the current U.S. administrative approach to data protection and the FTC's central role in it. Focusing on the FTC's broad consumer protection authority under Section 5(a) of the Federal Trade Commission Act of 1914, the nuts and bolts of every FTC data security action are explained. Part II provides an overview of two recent developments related to the FTC's data security efforts and analyzes their likely implications. Part III proposes a shift in regulatory focus, arguing that the FTC should promulgate a data security rule that identifies the contours of a lawful data security program. Although the Commission's procedural obligations are unique, the argument contends that a relatively expeditious rulemaking process is attainable. The analysis then identifies the factors that have prepared the FTC to promulgate such a data security rule and the regulatory advantages that may flow from it. To wrap up, the argument describes how the FTC can oversee the rulemaking process to ensure that its data security rule will survive judicial review.

I. THE U.S. ADMINISTRATIVE APPROACH TO DATA SECURITY

In contrast to other developed countries,[30] the United States does not regulate the use and collection of consumer data through a unitary framework.[31] Instead of passing an omnibus data protection law that empowers a single agency to oversee regulatory efforts, Congress has taken a sectoral approach, enacting a "patchwork"[32] of industry-specific data protection statutes.[33] Under this regime, many of the federal data protection laws regulate a specific category of consumer data utilized by a particular sector of the economy.[34]

---

[30] *See, e.g.*, Regulation 2016/479, of the European Parliament and of the Council of 27 Apr., 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; *Privacy Act 1988* (Cth) (Austl.); The Privacy Protection Law, 5741–1981, 35 LSI 136 (1980–81) (as amended) (Isr.).

[31] Neil M. Richards et. al, *Understanding American Privacy*, *in* RESEARCH HANDBOOK ON PRIVACY AND DATA PROTECTION LAW: VALUES, NORMS AND GLOBAL POLITICS (Gloria Gonzalez Fuster, Rosamunde van Brakel & Paul De Hert eds., forthcoming 2020), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3256918 ("American privacy law takes a *sectoral* or *sectorized* approach.").

[32] James P. Nehf, *Recognizing the Societal Value in Information Privacy*, 78 WASH. L. REV. 1, 58 (2003) (describing the U.S. approach to data regulation as a "patchwork of sector-specific privacy laws"); *see also* Solove & Hartzog, *supra* note 27, at 587 ("[p]rivacy law in the United States has developed in a fragmented fashion and is currently a hodgepodge of various" legal mechanisms).

[33] *See* Ryan Moshell, … *And Then There Was One: The Outlook for a Self-Regulatory United States Amidst a Global Trend Toward Comprehensive Data Protection*, 37 TEX. TECH L. REV. 357, 372 (2005) ("[T]he United States has always leaned on a sectoral approach [to data protection] under which … highly specific legislation merely tempers industry rather than directing it."); Reidenberg, *supra* note 26, at 877 (noting that in America, data "privacy is protected only through an amalgam of narrowly targeted rules").

[34] *See, e.g.*, Solove & Hartzog, *supra* note 27, at 587 ("[P]rivacy law in the United States is sectoral, with

For example, certain types of sensitive consumer health data are protected under the Health Insurance Portability and Accountability Act (HIPAA).[35] The Gramm-Leach-Bliley Act (GLBA) regulates specific types of financial information,[36] while the Fair Credit Reporting Act focuses on consumer credit reports.[37] The Children's Online Privacy Protection Act (COPPA) protects the online privacy interests of children twelve and under.[38] Other federal statutes address the privacy of video rental and sale records, cable communications, driving records, and consumer telephone numbers.[39] And alongside this matrix of federal laws, there is also a separate patchwork of state data security laws that covered companies must comply with.[40]

The United States' piecemeal approach to regulating data security has both advantages and drawbacks. A sector-focused *modus operandi* permits greater context specificity, injecting regulations with a more nuanced take on the unique data security issues that particular industries face.[41] In addition, government officials and industry representatives suggest that the current framework enables U.S. industries to maintain an impressive pace of technological innovation.[42] Yet

---

different laws regulating different industries and economic sectors.").

[35] *See* Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, 110 Stat. 1936 (codified as amended in scattered titles of U.S.C.). Health Insurance Portability and Accountability Act (HIPAA) is administered by the Department of Health and Human Services.

[36] Pub. L. No. 106-102, 113 Stat. 1338 (1999) (codified as amended in scattered sections 12, 15 U.S.C.). The Gramm-Leach-Bliley Act (GLBA) is jointly administered by several agencies, including the FTC and Consumer Financial Protection Bureau (CFPB). *See* Solove & Hartzog, *supra* note 27, at 602 n.71.

[37] Pub. L. No. 91-508, § 601, 84 Stat. 1114 (1970) (codified as amended primarily in 15 U.S.C. § 1681s (2012)). The Fair Credit Reporting Act (FCRA) is administered by both the CFPB and the FTC. *See* Solove & Hartzog, *supra* note 27, at 645–46.

[38] *See* 15 U.S.C. §§ 6501–6505 (2012). For more information on COPPA and the data security obligations that it imposes, see Solove & Hartzog, *supra* note 27, at 646–47.

[39] *See* Video Privacy Protection Act of 1988, Pub. L. No. 100-618, 102 Stat. 3195 (codified as amended at 18 U.S.C. §§ 2710–2711 (2012)); Cable Communications Policy Act of 1984, Pub. L. No. 98-549, 98 Stat. 2779 (codified as amended in scattered sections of 47 U.S.C.); Driver's Privacy Protection Act of 1994, Pub. L. No. 103-322, 108 Stat. 2099 (codified as amended in 18 U.S.C. §§ 2721–2725 (2012)); Telephone Consumer Protection Act of 1991, Pub. L. No. 102-243, 105 Stat. 2394 (codified as amended in 47 U.S.C. § 227 (2012)).

[40] *See, e.g.*, CAL. CIV. CODE § 1798.81.5 (West 2009) ("[A] business that owns or licenses personal information about a California resident [must] implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use, modification, or disclosure."); OR. REV. STAT. ANN. §§ 646A.622(1)–(2) (West 2011) ("Any person that owns, maintains or otherwise possesses data that includes a consumer's personal information that is used in the course of the person's business, vocation, occupation or volunteer activities must develop, implement and maintain reasonable safeguards to protect the security, confidentiality and integrity of the personal information.").

[41] *See, e.g.*, Richards et al., *supra* note 31, at 2 (discussing the pros and cons of the American privacy and data security regulatory schemata).

[42] *See* Natasha Singer, *Data Protection Laws, an Ocean Apart*, N.Y. TIMES (Feb. 2, 2013), https://www.nytimes.com/2013/02/03/technology/consumer-data-protection-laws-an-ocean-apart.html (quoting Kevin

the U.S. approach inevitably leads to gaps in coverage.[43] High-profile sectors of the economy, such as e-commerce, social media, smartphone apps, and Internet search engines, all lack specifically tailored data protection statues.[44] Although these industries do not go unregulated,[45] the conspicuous absence of particularized data protection laws in these increasingly pivotal industries weakens the entirety of the federal regulatory scheme.[46] Although public officials in the executive and legislative branches have proposed the adoption of comprehensive data security laws,[47] these attempts have failed to gain significant traction.[48]

A. The Federal Trade Commission: America's Primary Data Regulator

From this hodgepodge of data security regulation, the Federal Trade Commission has emerged as the "de facto" data protection authority.[49] Using its broad statutory authority to protect consumers against "unfair or deceptive acts or practices,"[50] the FTC has distinguished itself in the data security landscape.[51]

Richards, senior vice president of federal government affairs at TechAmerica, stating "[i]t's not wise to have an overly broad, prescriptive, one-size-fits-all approach that that would hinder or undermine the ability of companies to innovate in a global economy").

[43] *See* Andrea M. Matwyshyn, *Material Vulnerabilities: Data Privacy, Corporate Information Security, and Securities Regulation*, 3 BERKLEY BUS. L. J. 129, 169–70 (2005) ("[C]reating enclaves of superior data security for data related to children online, some financial information, and some health data will not alleviate the weak information security in other parts of the system and will not substantially diminish information crime.").

[44] *See* Cameron F. Kerry, *Why Protecting Privacy Is a Losing Game Today–and How To Change the Game*, BROOKINGS INST. (July 12, 2018), https://www.brookings.edu/research/why-protecting-privacy-is-a-losing-game-today-and-how-to-change-the-game/.

[45] As will be explained below, the Federal Trade Commission is authorized to regulate data security under Section 5 of the Federal Trade Commission Act of 1914. *See* 15 U.S.C. § 45 (2012).

[46] *See* Matwyshyn, *supra* note 43, at 170 ("[T]he lowest common security denominator determines the security of the system as a whole."); Lior Jacob Strahilevitz, *Toward a Positive Theory of Privacy Law*, 126 HARV. L. REV. 2010, 2011–12 (2013) ("The sectoral U.S. approach, which lacks an effective catch-all provision, renders American law both reactive and slow to react.").

[47] In 2012, the Obama Administration enumerated a "Consumer Privacy Bill of Rights" to be used as a "blueprint for privacy in the information age." *See* OFFICE OF THE WHITE HOUSE, CONSUMER DATA PRIVACY IN A NETWORKED WORLD: A FRAMEWORK FOR PROTECTING PRIVACY AND PROMOTING INNOVATION IN THE GLOBAL DIGITAL ECONOMY (2012). For legislative initiatives, see, e.g., Consent Act, S. 2369, 115th Cong. § 2 (2018) and Commercial Privacy Bill of Rights Act, S. 799, 112th Cong. §§ 3(6), 202(b), 501(a) (2011).

[48] *See, e.g.*, Grant Gross, *Cybersecurity Bill Fails in U.S. Senate*, COMPUTERWORLD (Nov. 14, 2012, 7:48 PM), http://www.computerworld.com/s/article/9233656/Cybersecurity_bill_fails_in_U.S._Senate.

[49] *See* Steven Hetcher, *The De Facto Federal Privacy Commission*, 19 J. MARSHALL J. COMPUTER & INFO. L. 109, 131 (2000) ("[T]he FTC is fairly viewed as a nascent, de facto federal privacy commission."); *see also* Hartzog & Solove, *supra* note 10, at 2236 ("[T]he FTC has evolved into the broadest and most powerful data protection agency in the United States.").

[50] 15 U.S.C. § 45(a)(1) (2012).

[51] *See* Gerard M. Stegmaier & Wendell Bartnick, *Psychics, Russian Roulette, and Data Security: The FTC's Hidden Data Security Requirements*, 20 GEO. MASON L. REV. 673, 674 (2013) ("Given the lack of a

Unlike other consumer protection agencies, whose efforts are limited to specified sectors of the American economy, the FTC can regulate digital security across a wide variety of industries.[52] And the FTC has tangible results to show for it: Since 2002, the Commission has brought over sixty data security enforcement actions.[53] These enforcement actions have alleged both unfair and deceptive data security practices, and have largely resulted in settlement agreements that impose remedial measures on offending entities.[54] Although commentators often evaluate the effectiveness of FTC data security regulation,[55] there is little debate concerning the Commission's authoritative stature in the field.

The subsections below will provide an overview of the FTC's authority in the data security regulatory environment. In Part I.A.1, the historical underpinnings of the FTC's consumer protection authority are outlined. Next, in Part I.A.2, the requisite elements that must support every FTC determination on data security are described. Last, Part I.A.3 explains the Commission's authority to bring enforcement proceedings.

1. A Brief Survey of the FTC's Consumer Protection Authority

Conceived in the throes of anti-business sentiment, the Federal Trade Commission was established by the Federal Trade Commission Act of 1914 (the "FTC Act").[56] Armed with substantial congressional authority, the FTC set out on its herculean mission: to "protect consumers and promote competition."[57] In its infancy, the FTC's sole task was to reign in monopolies and enforce fair

comprehensive federal regulatory scheme … it is not surprising that the Federal Trade Commission has begun requiring reasonable data security for entities not covered by existing, industry-specific federal regulations.").

[52] *See id.*; *see also* 15 U.S.C. § 45(a)(2) (2012) (providing the FTC with enforcement authority over "persons, partnerships, or corporations," subject to several exceptions).

[53] *See* FED. TRADE COMM'N, PRIVACY & DATA SECURITY UPDATE (2017): AN OVERVIEW OF THE COMMISSION'S ENFORCEMENT, POLICY INITIATIVES, AND CONSUMER OUTREACH AND BUSINESS GUIDANCE IN THE AREAS OF PRIVACY AND DATA SECURITY 4 (2017) (providing a recap of FTC data security enforcement actions).

[54] *See, e.g.*, Consent Order at 5, HTC Am. Inc., No. C-4406 (F.T.C. July 2, 2013); Consent Order at 4, Google Inc., No. C-4336 (F.T.C. Oct. 13, 2011).

[55] *Compare, e.g.*, Hartzog & Solove, *supra* note 10, at 2236 ("[T]he FTC has evolved into the broadest and most powerful data protection agency in the United States."), *with, e.g.*, Michael D. Scott, *The FTC, the Unfairness Doctrine, and Data Security Breach Litigation: Has the Commission Gone Too Far?*, 60 ADMIN. L. REV. 127, 183 (2008) (arguing that the FTC does not provide meaningful notice of what constitutes unfair data security practices).

[56] *See, e.g.*, Marc Winerman, *The Origins of the FTC: Concentration, Cooperation, Control, and Competition*, 71 ANTITRUST L.J. 1 (2003) (providing an in-depth review of the FTC's founding).

[57] *See* Federal Trade Commission Act of 1914, Pub. L. No. 63-203, 38 Stat. 717 (codified as amended at 15 U.S.C. § 45(a) (2012)).

competition.[58] Yet in the mid-1930s, amid growing public concern over the dangers of false advertising,[59] and on the heels of Supreme Court decisions narrowing the reach of the FTC Act,[60] Congress extended the FTC's mandate to explicitly encompass consumer protection.[61] Under Section 5(a) of the FTC Act, Congress provided the FTC with broad authority to "prevent persons, partnerships or corporations … from using … unfair or deceptive acts or practices in commerce."[62] In the nearly eighty years since, the FTC has used its Section 5(a) authority to enforce "unfair" and "deceptive" business practices in an impressive array of fields, including advertising,[63] packaging and labeling,[64] product warranties,[65] and consumer privacy.[66]

---

[58] *See* Federal Trade Commission Act of 1914, Pub. L. No. 63-203, § 5, 38 Stat. 717, 719 (codified as amended at 15 U.S.C. § 45(a) (2012)) (declaring "[u]nfair methods of competition in commerce" as unlawful). The FTC's Bureau of Competition continues to carry out this mission today.

[59] *See, e.g.*, CHRIS J. HOOFNAGLE, FEDERAL TRADE COMMISSION PRIVACY LAW AND POLICY 32–37 (2016) (discussing the proliferation of dangerous products in commerce, the misleading nature of their advertising, and how attendant public concern helped catalyze the Wheeler-Lea Act).

[60] *See* FTC v. Raladam Co., 283 U.S. 643, 654 (1931) (holding that unless a respondent's unfair acts or practices were proved to have injured actual or potential competitors, the FTC was powerless to prevent their use, irrespective of their injurious effect on the public); FTC v. Gratz, 253 U.S. 421, 427 (1920) ("The words 'unfair method of competition' are not defined by the statute and their exact meaning is in dispute. It is for the courts, not the commission, ultimately to determine as a matter of law what they include.").

[61] *See* Wheeler-Lea Act of 1938, Pub. L. No. 75-447, § 5, 52 Stat. 111, 111 (1938) (codified as amended at 15 U.S.C. § 45(a) (2012)); H.R. REP. NO. 75-1613, at 3 (1937) ("[T]his amendment makes the consumer, who may be injured by an unfair trade practice, of equal concern, before the law, with the merchant or manufacturer injured by the unfair methods of a dishonest competitor.").

[62] Wheeler-Lea Act § 5, 52 Stat. at 111. Regulated entities under the FTC Act include persons, partnerships and corporations, with some notable exceptions. *See* 15 U.S.C. § 45(a)(2) (2012) (exceptions include banks, savings and loan institutions, federal credit unions, and common carriers, among others). The Magnuson-Moss Warranty–Federal Trade Commission Improvements Act expanded the mandate to also include acts or practices "in or affecting commerce." *See* Pub. L. No. 93-637, § 201, 88 Stat. 2183, 2193 (1975) (codified as amended at 15 U.S.C. § 45(a) (2012)).

[63] *See, e.g.*, Warner-Lambert Co. v. FTC, 562 F.2d 749 (D.C. Cir. 1977) (affirming the FTC's authority to declare a false advertisement as deceptive); Press Release, Fed. Trade Comm'n, Internet Marketers of Dietary Supplement and Skincare Products Banned from Deceptive Advertising and Billing Practices (Nov. 15, 2017), https://www.ftc.gov/news-events/press-releases/2017/11/internet-marketers-dietary-supplement-skincare-products-banned.

[64] *See, e.g.*, Fair Packaging and Labeling Act, 15 U.S.C. §§ 1451–1461 (2012) (directing the FTC to issue regulations concerning consumer commodity labels in order to prevent consumer deception); Press Release, Fed. Trade Comm'n, Nordstrom, Bed Bath & Beyond, Backcountry.com, and J.C. Penney to Pay Penalties Totaling $1.3 Million for Falsely Labeling Rayon Textiles as Made of "Bamboo" (Dec. 9, 2015), https://www.ftc.gov/news-events/press-releases/2015/12/nordstrom-bed-bath-beyond-backcountrycom-jc-penney-pay-penalties.

[65] *See e.g.*, Magnuson-Moss Warranty Act, 15 U.S.C. §§ 2301–2308 (2012) (directing the FTC to issue regulations concerning consumer warranties); Press Release, Fed. Trade Comm'n, BMW Settles FTC Charges that Its MINI Division Illegally Conditioned Warranty Coverage on Use of Its Parts and Service (Mar. 19, 2015), https://www.ftc.gov/news-events/press-releases/2015/03/bmw-settles-ftc-charges-its-mini-division-illegally-conditioned.

[66] *See, e.g.*, FTC v. Wyndham Worldwide Corp., 799 F.3d 236, 243 (3d Cir. 2015) (affirming the FTC's authority to regulate data security).

Congress notably declined to give the terms "unfair" and "deceptive" static meanings, and instead deferred this ongoing interpretive task to the FTC, which was more nimble and focused in addressing evolving consumer problems.[67] In carrying out this interpretive function, the FTC has provided the regulated community with notice of what constitutes "unfair or deceptive acts or practices"[68] through a variety of means, including non-binding guidance documents,[69] case-by-case enforcement proceedings,[70] and the promulgation of Trade Regulation Rules (TRRs).[71] The following subsection will briefly trace the development of the "deception" and "unfairness" prongs in order to provide a framework by which the FTC exerts its Section 5(a) authority in the data security context.

2. Section 5: Unfair or Deceptive Acts or Practices

When Congress amended Section 5 of the FTC Act in 1938, it intentionally declined to define the critical terms "unfair" and "deceptive," and instead delegated this task to the FTC.[72] To this day, the FTC continues to develop the boundaries of what constitutes "unfair" and "deceptive" business practices in order to better protect consumers and provide fair notice to regulated entities.[73]

The FTC's most comprehensive attempt to define "deceptive" business practices is contained within the 1983 FTC Policy Statement on Deception.[74]

---

[67] *See, e.g.*, HOOFNAGLE, *supra* note 59, at 119–20 (noting that "Congress affirmatively made a policy decision to choose vague language in [the FTC and Wheeler-Lea Acts] because business practices and technology were constantly evolving, causing new problems that Congress could not quickly act to remedy"); *see also* FTC v. Raladam Co., 283 U.S. 643, 648 (1931) (noting that the term unfairness "belongs to that class of phrases which do not admit of precise definition, but the meaning and application of which must be arrived at by what this court elsewhere has called 'the gradual process of judicial inclusion and exclusion'" (quoting Davidson v. City of New Orleans, 96 U.S. 97, 104 (1878))); Eugene R. Baker & Daniel J. Baum, *Section 5 of the Federal Trade Commission Act: A Continuing Process of Redefinition*, 7 VILL. L. REV. 517, 519 (1962) ("[Section 5] cannot be defined in terms of constants. More broadly, it is a recognition of an ever-evolving commercial dexterity and the personal impact of economic power as important dimensions of trade.").

[68] 15 U.S.C. § 45(a)(1) (2012).

[69] *See, e.g.*, *Stick with Security: A Business Blog Series*, FED. TRADE COMMISSION (Oct. 2017), https://www.ftc.gov/tips-advice/business-center/guidance/stick-security-business-blog-series.

[70] *See, e.g.*, Complaint, Eli Lilly & Co., 133 F.T.C. 763 (2002) (charging pharmaceutical company with deceptive business practice in breaking privacy agreement and disclosing customers' personal information).

[71] *See, e.g.*, FTC Funeral Industry Practices Rule, 16 C.F.R. § 453 (2018) (outlining unfair and deceptive business practices in the funeral industry).

[72] *See supra* note 67.

[73] *See, e.g.*, Solove & Hartzog, *supra* note 27, at 628–43 (tracing the development of the FTC's deception and unfairness theories in the digital privacy context).

[74] *See* Letter from James C. Miller III, Fed. Trade Comm'n Chairman, to John D. Dingell, Chairman, House Comm. on Energy and Commerce (Oct. 14, 1983) [hereinafter Policy Statement on Deception]. The Policy Statement on Deception is also appended to Cliffdale Assocs., Inc., 103 F.T.C. 110, 174 (1984).

The Statement supplied the Commission's view that a deception claim must allege a (1) material (2) representation, omission, or practice (3) that is likely to mislead a consumer who is acting reasonably in the circumstances.[75] Therefore, in determining whether a particular act or practice is deceptive, the FTC has indicated that the conduct in question need not actually mislead consumers; a likelihood of deception is sufficient.[76] Moreover, the FTC will consider the allegedly deceptive conduct from the perspective of an ordinary and prudent consumer.[77] Although the Policy Statement on Deception is a nonlegislative rule that the FTC could abandon at any time,[78] it has proven to be a robust test that continues to inform agency enforcement actions.[79]

In tandem, Section 5(a) of the FTC Act authorizes the Commission to administer the prohibition of "unfair" business practices, which are legally distinct from "deceptive" ones.[80] Initially, the FTC developed the elements of an unfair business practice principally through agency adjudication.[81] After unsuccessfully experimenting with an unfairness standard that considered whether the act in question was "immoral, unethical, oppressive, or unscrupulous," the Commission sought to reorganize its conception of unfairness.[82] The resulting document, known as the 1980 Policy Statement on

---

[75] *See* Policy Statement on Deception, *supra* note 74 ("[T]he Commission will find deception if there is a representation, omission or practice that is likely to mislead the consumer acting reasonably in the circumstances, to the consumer's detriment.").

[76] *See id.* ("The issue is whether the act or practice is likely to mislead, rather than whether it causes actual deception.").

[77] *See id.* ("The Commission believes that to be deceptive the representation, omission or practice must be likely to mislead reasonable consumers under the circumstances.").

[78] *See* 5 U.S.C. § 553(b)(A) (2012) (stating that notice-and-comment requirements do not apply "to interpretive rules, [and] general statements of policy"); *see also* HOOFNAGLE, *supra* note 59, at 123 ("At any time, the Commission could abandon the Deception Statement formally.").

[79] *See*, *e.g.*, Complaint, Petco Animal Supplies, Inc., 139 F.T.C. 102, 104–05 (2005) (alleging defendant engaged in unfair or deceptive business practice when it failed to provide appropriate security); Complaint, Microsoft Corp., 134 F.T.C. 709, 714–15 (2002) (charging company with deceptive business practice for collecting information beyond what was provided for in its privacy policy).

[80] 15 U.S.C. § 45(a) (2012).

[81] *See* FTC v. Wyndham Worldwide Corp., 799 F.3d 236, 243 (3d Cir. 2015) (Finding that in the decades after the passing of the Wheeler-Lea Act, "the FTC interpreted the unfair-practices prong primarily through agency adjudication"). Agencies are permitted to exercise discretion when choosing to proscribe policy either through rulemaking or adjudication. *See* SEC v. Chenery Corp. (*Chenery II*), 332 U.S. 194, 202 (1947).

[82] *See*, *e.g.*, Statement of Basis and Purpose of Trade Regulation Rule, Unfair or Deceptive Advertising and Labeling of Cigarettes in Relation to the Health Hazards of Smoking, 29 Fed. Reg. 8324, 8355 (July 2, 1964) (to be codified at 16 C.F.R. pt. 408). Hoofnagle notes that after the FTC prescribed the "cigarette rule" unfairness criteria, it "began using unfairness in a number of rulemaking efforts, against politically powerful businesses and in situations with more moral ambiguity," resulting in mixed regulatory success. HOOFNAGLE, *supra* note 59, at 131.

Unfairness, enumerated definite criteria that the FTC would thereafter look to when singling out an act or practice as unfair.[83]

In 1994, Congress codified the unfairness elements into Section 5(n) of the FTC Act.[84] Section 5(n) reads:

> The Commission shall have no authority … to declare unlawful an act or practice on the grounds that such an act or practice is unfair unless the act or practice causes or is likely to cause substantial injury to consumers which is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or competition. In determining whether an act or practice is unfair, the Commission may consider established public policies as evidence to be considered with all other evidence. Such public policy considerations may not serve as a primary basis for such determination.[85]

Thus, in any adjudicatory or rulemaking proceeding concerning unfairness, the FTC must show that the act or practice in question (1) causes or is likely to cause substantial injury to consumers (2) that is not reasonably avoidable by consumers themselves and (3) not outweighed by countervailing benefits to consumers or competition.[86] As such, Section 5(n) has served to limit the FTC's authority to declare certain acts or practices unlawful on unfairness grounds.[87] If the Commission fails to convincingly prove the three elements in a rulemaking or adjudicatory proceeding, it risks judicial rebuke.[88]

---

[83] Letter from Michael Pertschuk, Chairman, Fed. Trade Comm'n, and Paul Rand Dixon, Comm'r, Fed. Trade Comm'n, to Wendell H. Ford, Chairman, House Commerce Subcomm. on Commerce, Sci. &Transp. (Dec. 17, 1980), https://www.ftc.gov/public-statements/1980/12/ftc-policy-statement-unfairness [hereinafter Policy Statement on Unfairness].

[84] *See* Federal Trade Comission Act Amendments of 1994, Pub. L. No. 103–312, § 9, 108 Stat. 1691, 1695 (codified as amended at 15 U.S.C. § 45(n) (2012)). In codifying the unfairness elements, Congress slightly modified the 1980 Policy Statement on Unfairness, eliminating the public policy factor as an independent basis sufficient to support a claim of unfairness. *Compare* Policy Statement on Unfairness, *supra* note 83, *with* 15 U.S.C. § 45(n) (2012).

[85] 15 U.S.C. § 45(n) (2012).

[86] *See id.*

[87] *See* Solove & Hartzog, *supra* note 27, at 638 ("In many ways, the FTC's unfairness jurisdiction is quite limited.").

[88] *See* 15 U.S.C. § 45(n) (2012) ("The Commission shall have no authority under … section [45] or section 57a of this title to declare unlawful an act or practice on the grounds that such an act or practice is unfair unless the act or practice causes or is likely to cause substantial injury to consumers which is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition.").

Of the criteria, substantial consumer injury "carries the greatest weight in an unfairness analysis."[89] According to the FTC, substantial injury can result from acts or practices "causing a very severe harm to a small number" of people or a "small harm to a large number [of] people."[90] Typically, speculative and subjective harms are rejected in favor of more concrete harms related to financial, health, and safety risks.[91]

The second element, practical unavoidability, seeks to enshrine effective consumer decision-making, particularly when "seller behavior … unreasonably creates or takes advantage of an obstacle to the free exercise of consumer decision-making."[92] Finally, the countervailing benefits element ensures that unfair business practices are "injurious in [their] net effects."[93] When balancing the allegedly unfair practice with countervailing benefits, the FTC will consider strains that may be imposed by a remedy, including the costs to businesses and consumers, as well as "burdens on society in general in the form of increased paperwork, increased regulatory burdens on the flow of information [and] reduced incentives to innovation and capital formation…."[94]

3. Enforcing Violations of Section 5

To give teeth to the FTC's bite, Congress endowed the Commission with two means of enforcing violations of Section 5(a): administrative proceedings[95] and judicial enforcement in federal district court.[96]

After conducting an investigation,[97] the Commission may elect to enforce an allegedly unfair or deceptive practice via administrative proceeding, which it

---

[89] Marcia Hofmann, *Federal Trade Commission Enforcement of Privacy*, *in* PROSKAUER ON PRIVACY: A GUIDE TO PRIVACY AND DATA SECURITY LAW IN THE INFORMATION AGE § 4:1.2 (Kristen J. Mathews ed., 2016).

[90] Int'l Harvester Co., 104 F.T.C. 949, 1064 (1984).

[91] *Id.* at 1073 ("The Commission is not concerned with trivial or merely speculative harms.").

[92] *Id.* at 1074.

[93] *Id.* at 1073.

[94] *Id.* at 1073–74.

[95] *See* 15 U.S.C. § 45(b) (2012).

[96] *See id.* § 53(a)–(b).

[97] *See id.* § 46(a) (providing the FTC with the power to "gather and compile information concerning, and to investigate from time to time the organization, business, conduct, practices, and management of any person, partnership, or corporation engaged in or whose business affects commerce").

commences by drafting an administrative complaint.[98] The subject of an FTC complaint can either settle[99] or contest the proceeding.[100]

In the data security context, nearly every complaint has resulted in settlement.[101] FTC settlement agreements, known as consent orders, cannot impose first-step financial penalties and do not require the regulated entity to admit liability.[102] However, they do compel the settling party to implement prospective remedial measures, typically in the form of a revised data security program.[103] If the FTC determines that a settling party has failed to comply with a consent order, only then can it levy civil penalties for each violation.[104]

If the subject of a complaint decides to challenge the FTC's determination, it is afforded the opportunity to do so in a hearing before an administrative law judge (ALJ).[105] After the ALJ issues an initial decision, either party may appeal to the active commissioners,[106] who may review the ALJ's findings of fact and

---

[98] *See id.* § 45(b). Before filing a complaint, the active FTC commissioners must vote on the matter, taking into account the merits of the claim and whether enforcement would be in the public interest. *See id.* ("[I]f it shall appear to the Commission that a proceeding … would be in the interest of the public," it may initiate one); 16 C.F.R. § 3.11(a) (2018) ("[A]n adjudicative proceeding is commenced when an affirmative vote is taken by the Commission to issue a complaint.").

[99] *See* 15 U.S.C. § 45(m)(3) ("The Commission may compromise or settle any action for a civil penalty if such compromise or settlement is accompanied by a public statement of its reasons and is approved by the court.").

[100] *See id.* § 45(b).

[101] *See* Solove & Hartzog, *supra* note 27, at 610–11 (noting that as of 2014, the FTC had "issued over 170 privacy-related complaints against companies. Yet virtually every complaint has either been dropped or settled"). *But see* FTC v. Wyndham Worldwide Corp., 799 F.3d 236 (3d Cir. 2015). For a comprehensive review of the factors motivating this result, see Solove & Hartzog, *supra* note 27, at 611–13 (citing the financial and reputational costs associated with negotiation and litigation, agency deference afforded by reviewing courts, and the ability to settle without admitting wrongdoing).

[102] *See* 16 C.F.R. § 2.32 (2018) (a consent order "may state that the signing thereof is for settlement purposes only and does not constitute an admission by any party that the law has been violated as alleged in the complaint").

[103] *See, e.g.*, Order, BJ's Wholesale Club, Inc., 2005 WL 2395788 at *3 (F.T.C. Sept. 20, 2005) (No. 042-3160) ("It is so ordered that Respondent … establish and implement, and thereafter maintain, a comprehensive information security program that is reasonably designed to protect the security, confidentiality, and integrity of personal information collected from or about consumers.").

[104] *See* 15 U.S.C. § 45(l) (2012) (authorizing the Commission to obtain civil penalties of up to $10,000 per violation of a final order); 16 C.F.R. § 1.98(c) (2019) (raising the per-violation penalty to $42,530 to account for inflation). Because each day of noncompliance is considered a violation, these civil penalties can quickly add up to substantial sums. *See, e.g.*, Press Release, Fed. Trade Comm'n, LifeLock to Pay $100 Million to Consumers to Settle FTC Charges It Violated 2010 Order (Dec. 17, 2015), https://www.ftc.gov/news-events/press-releases/2015/12/lifelock-pay-100-million-consumers-settle-ftc-charges-it-violated.

[105] *See* 15 U.S.C. § 45(b); 16 C.F.R. §§ 3.42, 3.51 (2018).

[106] Here, the "Commission" refers to the five individual commissioners of the FTC, who are appointed by the President. *See Commissioners*, FED. TRADE COMMISSION, https://www.ftc.gov/about-ftc/commissioners (last visited Oct. 11, 2018).

conclusions of law.[107] Once the commissioners enter a final decision, the FTC issues a cease and desist order against the regulated entity.[108] Yet the subject of the order has one last opportunity at a favorable outcome: It may challenge the Commission's final decision in the appropriate federal appellate court.[109]

Alternatively, under the judicial enforcement model, the FTC may file complaints alleging unfair or deceptive business practices directly in federal district court, seeking temporary restraining orders, preliminary injunctions, or consumer redress.[110] Much like the administrative model, many of these judicial proceedings result in settlement,[111] whereby the FTC lacks the authority to impose civil penalties unless the settlement order is violated.[112]

In addition to the regulatory powers outlined above, the FTC has one final means of enforcing unfair or deceptive data security acts or practices: rulemaking. The coming Section will explore this critical function.

B. The FTC's Rulemaking Authority

Under Section 18 of the FTC Act, the Commission is empowered to promulgate rules that identify specific unfair or deceptive acts or practices.[113] These rules provide the regulated community notice of what constitutes an unfair or deceptive business practice, as well as a road map for successful

---

[107] *See* 16 C.F.R. §§ 3.52, 3.54.

[108] *See* 15 U.S.C. § 45(b) (2012) ("If upon such hearing the Commission shall be of the opinion that the method of competition or the act or practice in question is prohibited … it shall … issue … an order requiring [the party] to cease and desist from" the unfair or deceptive practice).

[109] *See id.* § 45(c). The appropriate federal appellate court has the "power to make and enter a decree affirming, modifying, or setting aside the order of the Commission, and enforcing the same to the extent that such order is affirmed." *Id.*

[110] *See id.* § 53(b). For examples of such complaints, see, e.g., First Amended Complaint for Injunctive and Other Equitable Relief, FTC v. Wyndham Worldwide Corp., No. CV 12-1365-PHX-PGR, 2013 WL 1222491, at *1 (D. Ariz. Mar. 25, 2013); Complaint for Injunctive and Other Equitable Relief, FTC v. Accusearch, Inc., No. 06-CV-105-D, 2007 WL 4356786, at *1 (D. Wyo. Sept. 28, 2007), *aff'd*, 570 F.3d 1187 (10th Cir. 2009).

[111] *See*, *e.g.*, Press Release, Fed. Trade Comm'n, Debt Brokers Settle FTC Charges They Exposed Consumers' Information Online (Apr. 13, 2015), https://www.ftc.gov/news-events/press-releases/2015/04/debt-brokers-settle-ftc-charges-they-exposed-consumers; Press Release, Fed. Trade Comm'n, ChoicePoint Settles Data Security Breach Charges; to Pay $10 Million in Civil Penalties, $5 Million for Consumer Redress (Jan. 26, 2006), https://www.ftc.gov/news-events/press-releases/2006/01/choicepoint-settles-data-security-breach-charges-pay-10-million.

[112] *See* 15 U.S.C. § 45(l).

[113] *See* 15 U.S.C. § 57a (2012) ("Authority of Commission to Prescribe Rules and General Statements of Policy"); *see also* Nat'l Petroleum Refiners Ass'n v. FTC, 482 F.2d 672, 698 (D.C. Cir. 1973) ("[T]he Federal Trade Commission is authorized to promulgate rules defining the meaning of the statutory standards of the illegality the Commission is empowered to prevent.").

compliance.[114] If the FTC finds that an entity is engaging in an unfair or deceptive act as defined by a legally binding trade regulation rule (TRR), it may pursue an enforcement action against the violator in an effort to obtain civil penalties or provide consumers with redress.[115] The FTC's rulemaking capacity can be bifurcated into two categories: nonlegislative and legislative.[116]

1. Nonlegislative Rules

As prescribed in the FTC Act, nonlegislative rules are "interpretive rules and general statements of policy with respect to unfair or deceptive practices."[117] Guidance documents, as they are commonly referred to, are unencumbered by the procedural constraints of notice-and-comment rulemaking.[118] Agency policy statements strive to "advise the public prospectively of the manner in which the agency proposes to exercise a discretionary power."[119] Interpretive rules reflect the agency's contemporaneous interpretation of its organic statute and lay out how the agency views its administrative function.[120] Indeed, regulated entities typically seek out guidance documents, as they may supply a relevant framework for compliance.[121] However, the influence of nonlegislative rules is not limitless: Agencies are not unilaterally bound by them[122] and reviewing courts are only obligated to give them deference according to their persuasive force.[123]

---

[114] *See* Stegmaier & Bartnick, *supra* note 51, at 710 ("Rulemaking likely is the best method for providing authoritative, detailed guidance so that entities know how to comply with the law.").

[115] *See* 15 U.S.C. § 45(m)(1)(A) ("The Commission may commence a civil action to recover a civil penalty in a district court of the United States against any person, partnership, or corporation which violates any rule under this subchapter respecting unfair or deceptive acts or practices…."); *id.* § 57b(a)–(b) ("If … any person, partnership, or corporation violates any rule under this subchapter respecting unfair or deceptive acts or practices" then the Commission may commence a civil action … "for relief … necessary to redress injury to consumers.").

[116] *See id.* § 57a(a)(1)(A)–(B).

[117] *Id.* § 57a(a)(1)(A).

[118] *See* 5 U.S.C. § 553(b)(A) (2012) ("[T]his subsection does not apply to interpretive rules, general statements of policy or rules of agency organization, procedure or practice.").

[119] U.S. DEP'T OF JUSTICE, ATTORNEY GENERAL'S MANUAL ON THE ADMINISTRATIVE PROCEDURE ACT 30 n.3 (1947).

[120] *See, e.g.*, Robert A. Anthony, *Interpretive Rules, Policy Statements, Guidances, Manuals, and the Like—Should Federal Agencies Use Them to Bind the Public?*, 41 DUKE L.J. 1311, 1325 (1992) ("An interpretive rule is an agency statement that was not issued legislatively and that interprets language of a statute … that has some tangible meaning.").

[121] *See, e.g.*, PETER L. STRAUSS ET AL., GELLHORN AND BYSE'S ADMINISTRATIVE LAW CASES AND COMMENTS 190 (11th ed. 2011) (discussing "the important benefits that guidance documents can bring"); Solove & Hartzog, *supra* note 27, at 626 ("Companies take the guidance in these materials seriously.").

[122] *See, e.g.*, Am. Mining Cong. v. Mine Safety & Health Admin., 995 F.2d 1106, 1111 (D.C. Cir. 1993) ("A non-legislative rule's capacity to have a binding effect is limited.").

[123] *See* Skidmore v. Swift & Co., 323 U.S. 134, 140 (1944) (holding that an administrative agency's interpretive rules deserve deference according to their persuasiveness); *see also* 5 U.S.C. § 552(a)(2) (2012)

In the context of data security, the FTC has provided the regulated public with a substantial body of nonlegislative guidance.[124] FTC data security guidance documents range from issue- and industry-specific data security compendiums,[125] to more generalized handbooks and resources that cut across business sectors.[126] For example, the FTC's 2016 *Protecting Personal Information: A Guide for Business* offers concrete steps that regulated entities can take to better protect their consumer data and avoid FTC enforcement action.[127]

While these guidance documents provide much-needed insight into the FTC's evolving conception of best practice, critics claim it is unclear exactly which recommendations the Commission will consider as mandatory components of a legally permissible data security program.[128] But such uncertainty is inherent.[129] As nonlegislative rules, data security guidance documents do not purport to carry the force of law.[130] Yet even without binding authority, these materials influence the security practices of attentive firms.[131] Thus, for companies in search of best practice guidance, FTC data security nonlegislative rules represent a meaningful yet incomplete source of interpretive aid in the pursuit of compliance.[132]

(stating that an agency's guidance documents may be "cited as precedent" if published); United States v. Mead Corp., 553 U.S. 218, 226–27 (2001) (holding that absent Congressional intent concerning the force of law, nonlegislative rules are not entitled to *Chevron* deference).

[124] For a full list of FTC data security guidance documents, see *Data Security*, FED. TRADE COMMISSION, https://www.ftc.gov/tips-advice/business-center/privacy-and-security/data-security (last visited Jan. 7, 2019).

[125] *See, e.g.*, *App Developers: Start with Security*, FED. TRADE COMMISSION, https://www.ftc.gov/tips-advice/business-center/guidance/app-developers-start-security (last visited Jan. 7, 2019); *Peer-to-Peer File Sharing: A Guide for Business*, FED. TRADE COMMISSION, https://www.ftc.gov/tips-advice/business-center/guidance/peer-peer-file-sharing-guide-business (last visited Jan. 7, 2019).

[126] *See, e.g.*, PRIVACY & DATA SECURITY UPDATE, *supra* note 53; FED. TRADE COMM'N, PROTECTING PERSONAL INFORMATION: A GUIDE FOR BUSINESS (2016) [hereinafter PROTECTING PERSONAL INFORMATION].

[127] Such steps deal with data inventory, physical and electronic security, authentication, firewalls, employee training, breach detection, proper data deletion and the creation of security incidence response plans. *See* PROTECTING PERSONAL INFORMATION, *supra* note 126.

[128] *See* Solove & Hartzog, *supra* note 27, at 626 (discussing common criticisms of the FTC's data security guidance documents); *see also* Justin Hurwitz, *Data Security and the FTC's UnCommon Law*, 103 IOWA L. REV. 1003, 1012 (2016) (criticizing the effectiveness of FTC data security guidance documents on grounds that firms will not seek them out organically, but will instead seek guidance from industry specific regulators, and local business and corporate law).

[129] *See generally* STRAUSS ET AL., *supra* note 121, at 190 (noting that when "agencies are limited in their ability to indicate acceptable approaches to meeting a standard in common contexts, [guidance-based] standards may carry … uncertainty").

[130] *See supra* notes 118, 122.

[131] *See* Solove & Hartzog, *supra* note 27, at 626 (arguing that "[c]ompanies take the guidance in [non-legislative rules] seriously").

[132] *See id.* (noting that despite a lack of clarity as to "which parts of [the FTC's guidance documents] are mandatory and which parts are simply best practices … these materials have weight").

2. Legislative Rules: The Magnuson-Moss Act & Trade Regulation Rules

The FTC also enjoys the authority to promulgate legislative rules that legally bind both agency and public actions.[133] Under the Magnuson-Moss Warranty–Federal Trade Commission Improvement Act,[134] the FTC may enact legislative rules "which define with specificity acts or practices which are unfair or deceptive acts or practices in or affecting commerce."[135] These rules, known as trade regulation rules (TRRs),[136] may also "include requirements prescribed for the purpose of preventing [unfair or deceptive] acts or practices."[137]

The procedural requirements imposed by Magnuson-Moss rulemaking[138] are unique in that they are greater than what is required under the Administrative Procedure Act's baseline notice-and-comment rulemaking,[139] yet less onerous than formal rulemaking.[140] Thus, Magnuson-Moss rulemaking falls into the relatively rare category of "hybrid" rulemaking.[141] A defining feature of Magnuson-Moss procedure is public participation, a principle that is interwoven throughout the administrative state.[142] For example, Magnuson-Moss

---

[133] *See* Nat'l Petroleum Refiners Ass'n v. FTC, 482 F.2d 672, 678, 698 (D.C. Cir. 1973); STRAUSS ET AL., *supra* note 121, at 110 ("If authorized by statute and adopted through the required procedures, regulations have legally binding effect on government and citizens alike, until displaced by statute or other validly adopted regulations.").

[134] Magnuson-Moss Warranty—Federal Trade Commission Improvement Act, Pub. L. No. 93–637, § 202, 88 Stat. 2183, 2193 (1975) (codified as amended at 15 U.S.C. §§ 45–46, 49–52, 56–57c, 2301–2312 (2012)).

[135] 15 U.S.C. § 57a(a)(1)(B) (2012). The provision reads in full:

> Except as provided in subsection (h) of this section, the Commission may prescribe … rules which define with specificity acts or practices which are unfair or deceptive acts or practices in or affecting commerce (within the meaning of section 45(a)(1) of this title), except that the Commission shall not develop or promulgate any trade rule or regulation with regard to the regulation of the development and utilization of the standards and certification activities pursuant to this section. Rules under this subparagraph may include requirements prescribed for the purpose of preventing such acts or practices.

[136] *See* FED. TRADE COMM'N, OPERATING MANUAL § 7.2.2 (1971) [hereinafter OPERATING MANUAL]. All existing TRRs may be found in Title 16 of the Code of Federal Regulations under subchapter D. *See* 16 C.F.R. §§ 408–460 (2018).

[137] 15 U.S.C. § 57a(a)(1)(B). When the FTC promulgates a legislative rule pertaining to competition, it need only adhere to notice-and-comment rulemaking procedure. *See* OPERATING MANUAL, *supra* note 136, § 7.4.

[138] *See* 15 U.S.C. § 57a(b) ("Procedures Applicable"); *id.* § 57a(c) ("Informal Hearing Procedure"); *id.* § 57a(d)(1) ("Statement of Basis and Purpose Accompanying Rule"); *see also* OPERATING MANUAL, *supra* note 136, § 7.3.2.

[139] *See* 5 U.S.C. § 553(b)–(e) (2012) (prescribing the procedural requirements of notice-and-comment rulemaking).

[140] *See id.* §§ 556–557 (prescribing the procedural requirements of formal rulemaking).

[141] *See* STRAUSS ET AL., *supra* note 121, at 129 n.3 (noting that the Federal Trade Commission Improvements Act of 1975 is one of the statutes that imposes "'hybrid' rulemaking processes").

[142] *See, e.g.*, William Funk, *Public Participation and Transparency in Administrative Law–Three*

rulemaking requires the FTC to "provide for an informal hearing" in which interested parties are entitled to present evidence and, if necessary, cross-examine witnesses.[143] In addition, the FTC must provide advanced notice of proposed rulemaking to Congress,[144] consider regulatory alternatives,[145] and make a determination that the allegedly unfair or deceptive activity is "prevalent."[146] The Commission is also obligated to publish a "statement of basis and purpose to accompany" the final TRR.[147] Finally, throughout the process, the FTC must compile a "rulemaking record" to be used in case of judicial review.[148]

The Magnuson-Moss Act also gives the FTC authority to meaningfully enforce TRRs.[149] If a regulated entity engages in one of the unfair or deceptive business practices identified by a TRR, the FTC may pursue the violator for civil penalties and consumer redress in a federal district court.[150] Because the FTC lacks authority to lead with civil penalties under its case-by-case adjudicatory enforcement model, this statutory authorization provides the FTC with a potent means of deterring noncompliance.[151]

To date, the FTC has yet to exercise its Magnuson-Moss rulemaking authority in the information security setting.[152] As such, regulated entities cannot look to a specific TRR when seeking to comply with the FTC's data security

---

Examples as an Object Lesson, 61 ADMIN. L. REV. 171, 172–77 (2009) (tracing the development of public participation in the administrative state).

143 *See* 15 U.S.C. § 57a(b)–(c).

144 *See id.* § 57a(b)(2)(B).

145 *Id.* § 57a(b)(1)(A).

146 *See id.* § 57a(b)(3).

147 *See id.* § 57a(d)(1). The Statement of Basis and Purpose must include "(A) a statement as to the prevalence of the acts or practices treated by the rule; (B) a statement as to the manner and context in which such acts or practices are unfair or deceptive; and (C) a statement as to the economic effect of the rule, taking into account the effect on small business and consumers." *Id.* § 57a(d)(1)(C).

148 *See id.* § 57a(e)(3)(A) (stating that a reviewing court may set aside a rule as unlawful if it "finds that the Commission's action is not supported by substantial evidence in the rulemaking record"). The rulemaking record must consist of the rule, its statement of basis and purpose, public hearing transcripts, written submissions, and "any other information which the Commission considers relevant to such rule." *Id.* § 57a(e)(1)(B).

149 *See id.* § 45(m)(1)(A) ("Civil Actions for Recovery of Penalties for Knowing Violations of Rules"); *id.* § 57b(a)(1).

150 *See id.* § 57b(a)(1).; *see also* OPERATING MANUAL, *supra* note 136, § 7.3.28.2 ("Enforcement of TRR's").

151 *See, e.g.*, Prepared Statement of the Fed. Trade Comm'n, Oversight of the Fed. Trade Comm'n, Comm. on Energy and Commerce at 6 (July 18, 2018) ("Section 5 does not provide for civil penalties, reducing the Commission's deterrent capability."); Stegmaier & Bartnick, *supra* note 51, at 706 (arguing that "the potentially large penalty for noncompliance … involving data security can dramatically affect a business, particularly small Internet companies whose entire business is based on data").

152 *See* HOOFNAGLE, *supra* note 59, at 56 ("[T]he FTC has not sought to promulgate rules for privacy").

requirements. The dominant narrative presumes that Magnuson-Moss rulemaking procedures are inefficient and overly time-consuming.[153] Moreover, critics believe that the rapid pace of digitalization will render any data security rule outdated upon promulgation.[154] While it is true that technology is progressing at a rapid pace, this reality does not necessarily preclude the articulation of a sensible and coherent rule-based data security standard.[155] The FTC's administrative flexibility and data security know-how suggest that the Commission is both well qualified and well suited to promulgate a rule. So too, the many benefits that may result from rulemaking stand to reinforce the FTC's mission of protecting U.S. consumers. Although the effort will be considerable, the FTC can and should use its Congressional rulemaking authority to codify the baseline rules of consumer data protection.

In the context of data security, the Federal Trade Commission has broad authority to enforce "unfair or deceptive acts or practices."[156] Both the FTC and Congress have narrowed the scope of unfairness and deception by disclosing and codifying certain elements that must back up any Section 5 action.[157] Since it entered the world of data security enforcement, the FTC has primarily policed inadequate practices through an informal adjudicatory model, entering into settlement orders with remedial force.[158] And although the FTC retains the authority to promulgate a rule-based data security standard under the FTC Act, it has repeatedly declined to do so.[159] As the next Part will show, recent developments in the FTC's enforcement efforts have altered the landscape, and suggest that a new approach may be forthcoming.

---

153 *See* Stegmaier & Bartnick, *supra* note 51, at 692 (calling Magnuson-Moss rulemaking a "potentially inefficient and time-consuming process"); *Prepared Statement of the Federal Trade Commission on Data Security: Hearing Before the Subcomm. on Commerce, Mfg., and Trade of the H. Comm. on Energy and Commerce*, 112th Cong. 11 (2011) (statement of Edith Ramirez, Comm'r, Fed. Trade Comm'n) ("[E]ffective consumer protection requires that the Commission be able to promulgate these rules in a more timely and efficient manner.").

154 *See, e.g.*, HOOFNAGLE, *supra* note 59, at 102 ("[I]f a general, online privacy rule-making were started, it simply would be stale by its implementation date").

155 *See* Stegmaier & Bartnick, *supra* note 51, at 713 ("The rapid rate of technological progress should be no bar to crafting definite, coherent [data security] regulations.").

156 15 U.S.C. § 45(a) (2012); *see also* FTC v. Wyndham Worldwide Corp., 799 F.3d 236, 240, 259 (3d Cir. 2015) ("We thus affirm the District Court's decision" that "the FTC has authority to regulate cybersecurity under the unfairness prong" of Section 5).

157 *See supra* Part I.A.2.

158 *See, e.g.*, Stegmaier & Bartnick, *supra* note 51, at 693 ("The FTC also typically requires entities subject to a consent order involving data-security matters to implement the data-security practices it announces in its consent orders.").

159 *See id.* (commenting on "the FTC's declination to use its existing rulemaking authority to clarify its data-security expectations").

II. RECENT FTC DEVELOPMENTS IN DATA SECURITY

Although the FTC has proved to be a competent data security regulator,[160] recent events have highlighted the need for a sensible shift in approach. To date, the FTC has cautiously enforced unlawful data security by issuing complaints and settling allegations of unfair and deceptive practices.[161] These complaints and settlement agreements, in combination with guidance documents and judicial opinions, form the FTC's privacy jurisprudence, which is recognized as the most influential federal regulatory force on data security.[162] Taken together, the Commission's jurisprudence provides regulated entities with legally adequate yet baseline fair notice of what constitutes an unfair or deceptive data security program.[163]

In 2016, the FTC entered a final order against the medical testing company LabMD for engaging in unfair data security practices.[164] In doing so, the Commission articulated a unique and innovative conception of "substantial consumer injury" in the data security context.[165] Two years later, the Eleventh Circuit vacated the Commission's final order against LabMD on the narrow grounds that it lacked the specificity required to enforce it.[166] The following Sections will recount these developments and lay out the FTC's regulatory landscape moving forward. Part II.A examines the data security administrative complaint filed against LabMD. Tracing the FTC's internal review of the complaint, the analysis highlights the Commission's newly articulated conception of data breach harms and the important role it will serve moving forward. Part II.B explores the Eleventh Circuit's rebuke of the final order entered against LabMD and the potential consequences that may result from the decision.

---

160 *See, e.g.*, Stuart L. Pardau & Blake Edwards, *The FTC, the Unfairness Doctrine, and Privacy by Design: New Legal Frontiers in Cybersecurity*, 12 J. BUS. & TECH. L. 227, 242 (2017) ("After almost 20 years of investigating and enforcing internet privacy, the Commission has prosecuted a significant number of data security cases, and in those cases evolved a set of privacy principles.").

161 *See, e.g.*, Solove & Hartzog, *supra* note 27, at 619 ("[T]he FTC's privacy cases nearly all consist of complaints and settlements").

162 *See id.* at 587 ("It is fair to say that today FTC privacy jurisprudence is the broadest and most influential regulating force on information privacy in the United States—more so than nearly any privacy statute or common law tort.").

163 *See* FTC v. Wyndham Worldwide Corp., 799 F.3d 236, 257 (3d Cir. 2015) (noting that "courts regularly consider materials that are neither regulations nor 'adjudications on the merits'" and "the FTC's expert views about the characteristics of a 'sound data security plan'" could provide legally sufficient notice to the regulated public).

164 *See* Final Order, LabMD, Inc., No. C-9357 (F.T.C. July 28, 2016) [hereninafter LabMD Final Order], *overruled by* LabMD, Inc. v. FTC, 894 F.3d 1221 (11th Cir. 2018).

165 *See infra* Part II.A.

166 *See LabMD, Inc.*, 894 F.3d at 1221.

A. LabMD at the FTC: Demystifying Consumer Data Breach Harms

In any civil action dealing with data breach liability, establishing injury is a critical threshold issue.[167] For example, if an individual consumer plaintiff wishes to bring a private claim in federal court, he must demonstrate, under Article III standing doctrine,[168] that he has suffered either an "actual"[169] injury or an "imminent" injury that is "certainly impending."[170] If the plaintiff cannot do so, as is often the case, his claim will be dismissed.[171] In this recurring scenario, the affected consumer is left with few meaningful opportunities to mend his data breach injury.[172]

---

[167] *See, e.g.*, Opinion of the Comission at 9, LabMD, Inc., No. C-9357, (F.T.C. July 29, 2016) [hereinafter LabMD Comission Opinion] (finding that in a data security proceeding, "[t]he central focus of any inquiry regarding unfairness is consumer injury"), *overruled by* LabMD, Inc. v. FTC, 894 F.3d 1221 (11th Cir. 2018); Solove & Citron, *supra* note 10, at 739 ("The defining issue in [a data breach] lawsuit will be harm").

[168] Private data breach litigation is often filed in federal court under diversity jurisdiction. *See* 28 U.S.C. § 1332(a)(1) (2012). Data breach litigation filed in state court is often removed to federal court under the federal Class Action Fairness Act. *See* 28 U.S.C. § 1332(d); *see also* Solove & Citron, *supra* note 10, at 750 (explaining how data breach claims are brought in federal court).

[169] *See* Monsanto Co. v. Geerston Seed Farms, 561 U.S. 139, 149 (2010) ("Standing under Article III of the Constitution requires that an injury be concrete, particularized, and actual or imminent; fairly traceable to the challenged action; and redressable by a favorable ruling.").

[170] *See* Clapper v. Amnesty Int'l USA, 133 S. Ct. 1138, 1147 (2013) ("'[T]hreatened injury must be 'certainly impending' to constitute injury in fact,' and '[a]llegations of possible future injury' are not sufficient." (citing Whitmore v. Arkansas, 495 U.S. 149, 158 (1990))) (emphasis omitted).

[171] *See* Solove & Citron, *supra* note 10, at 740 (highlighting "[t]he courts' refusal to recognize data-breach harms"); *see also, e.g.*, Beck v. McDonald, 848 F.3d 262, 276–77 (4th Cir. 2017) (declining to find standing when plaintiffs alleged enhanced risk of future identity theft and incurred actual costs in protecting against identity theft and credit devaluation); *In re* Zappos.com, Inc., Customer Data Sec. Breach Litig., 108 F. Supp. 3d 949, 958–59 (D. Nev. 2015) (dismissing case for failure to allege standing where 24 million consumer credit card numbers were stolen because plaintiffs did not show any misuse or unauthorized purchases). *But see* Spokeo, Inc. v. Robins, 136 S. Ct. 1540, 1549 (2016) (noting that the risk of "intangible harm" may constitute "concrete harm" if the intangible harm shares a "close relationship to a harm that has traditionally been regarded as providing a basis for a lawsuit in English or American courts"). And while the Supreme Court's recent decision in *Spokeo* may indicate that federal courts are altering their approach to data breach injuries, *Spokeo's* application has been irregular. *Compare* Attias v. Carefirst, Inc., 865 F.3d 620, 629 (D.C. Cir. 2017) (finding that plaintiffs successfully alleged a substantial risk of harm "simply by virtue of the hack and the nature of the data that the plaintiffs allege was taken"), *with* Whalen v. Michaels Stores, Inc., 689 Fed. App'x 89, 90–91 (2d Cir. 2017) (case dismissed for lack of standing when plaintiff failed to allege a plausible threat of future fraud). For more information on data breach litigation statistics, see Sasha Romanosky et al., *Empirical Analysis of Data Breach Litigation*, 11 J. EMPIRICAL LEGAL STUD. 74 (2014).

[172] Solove and Citron note that in data breach cases, "[t]he law has various tools to provide redress for injuries," including state "data-breach-notification laws, regulatory enforcement, and litigation." Solove & Citron, *supra* note 10, at 781. However, when litigation fails, they argue that data-breach-notification laws "do little to redress any injuries caused." *Id.* With regard to regulatory enforcement, they contend that it "can be effective," yet "is limited in its extensiveness, as regulatory agencies are only able to pursue a small number of cases." *Id.* at 782; *see also id.* ("[I]ndividuals often have little say in whether [regulatory] enforcement actions are brought, and they lack much participation in the process. Regulatory enforcement waxes and wanes as agency priorities and personnel change.").

In contrast to private actions, the FTC need not allege consumer data breach injuries sufficient to establish Article III standing. Instead, under Section 5(n) of the FTC Act, every FTC data security unfairness proceeding rests on a showing that the unfair data security practice in question "causes or is likely to cause substantial injury to consumers."[173] But in the digital context, establishing a legally cognizable injury is delicate.[174] And because nearly every FTC unfairness proceeding has ended in a settlement,[175] public understanding of the Commission's approach to recognizing consumer data breach harms has been limited to the vaguely worded allegations contained in administrative complaints.[176]

This changed in 2016. In an opinion reversing a lower ALJ dismissal, the three acting FTC Commissioners[177] provided novel and valuable insight into how the Commission views its burden of establishing "substantial injury" in the data security context.[178] Back in 2013, the FTC filed an administrative complaint against LabMD, a medical testing company.[179] In its complaint, the Commission alleged that LabMD's "failure to employ reasonable … measures to prevent unauthorized access to personal information" constituted "an unfair act or practice under" Section 5 of the FTC Act.[180] Specifically, LabMD had suffered a data breach in which various types of consumer medical data became publically available online.[181] Bucking the trend, LabMD chose not to settle.[182] In an ensuing decision, the FTC's administrative law judge dismissed the

---

[173] 15 U.S.C. § 45(n) (2012). Deception proceedings do not require any explicit showing of consumer injury. *See, e.g.*, Maureen K. Ohlhausen, Comm'r, Fed. Trade Comm'n, Speech at the Federal Communications Bar Association: Painting the Privacy Landscape: Informational Injury in FTC Privacy and Data Security Cases (Sept. 19, 2017) ("Substantial injury isn't a prong of the deception legal analysis.").

[174] *See, e.g.*, Solove & Citron, *supra* note 10, at 756 (noting that "[t]he nature of data-breach harms is a complex issue").

[175] *See* Solove & Hartzog, *supra* note 27, at 611 n.120 ("Of the 154 [privacy] complaints reviewed for this Article, only six had no accompanying settlement agreement."). For a discussion on the incentive structures that inform both the FTC and industry's proclivity for settlement, see Hurwitz, *supra* note 128.

[176] *See, e.g.*, Complaint at 5–6, Trendnet, Inc., No. C-4426 (F.T.C. Jan. 16, 2014) ("The exposure of sensitive information through respondent's [hacked] cameras increases the likelihood that consumers or their property will be targeted for theft or other criminal activity.").

[177] Although the FTC ought to have five commissioners, the opinion was adjudicated in July 2016, after former Commissioners Julie Brill and Joshua Wright had left the Commission but before their replacements had been sworn in. *See Former Commissioners*, FED. TRADE COMMISSION, https://www.ftc.gov/about-ftc/biographies/former-commissioners (last visited Oct. 31, 2018).

[178] LabMD Commission Opinion, *supra* note 167, at 9.

[179] *See id.* at 1.

[180] *Id.* at 5.

[181] *See id.* at 3 ("[A] third party informed respondent that its June 2007 insurance aging report … was available on a P2P network through Limewire, a P2P file sharing application.").

[182] *See* Order Designating Administrative Law Judge, LabMD, Inc., No. C-9357 (F.T.C. Aug. 29, 2013), *overruled by* LabMD, Inc. v. FTC, 894 F.3d 1221 (11th Cir. 2018).

complaint.[183] According to the ALJ, the Commission had failed to prove that LabMD's data security practices "caused" or were "likely to cause" "substantial consumer injury" as required by the unfairness elements of Section 5(n).[184] The ALJ interpreted the "likely to cause" requirement to mean "having a high probability of occurring or being true."[185] Looking to the facts, the ALJ concluded that the FTC had "proven the 'possibility' of harm, but not any 'probability' or likelihood of harm."[186]

Upon review, the three active FTC Commissioners unanimously rejected the ALJ's decision and entered a final order against LabMD.[187] In doing so, the Commissioners articulated two principles that embody the FTC's consumer-friendly approach to recognizing data breach harms.[188] First, the Commission explained that the "likely to cause" standard does not require "precise quantification" when showing that substantial consumer injury is probable.[189] Instead, the Commissioners indicated that proof of a "significant risk of injury" would satisfy the standard.[190] In determining whether a practice has caused "significant risk of injury," the Commissioners illustrated a sliding-scale approach that considers the "likelihood … of the injury occurring" alongside the "magnitude or seriousness of the injury if it does occur."[191] Thus, if the severity of potential injury is great, a lesser showing of probability may satisfy the "likely to cause substantial injury" requirement.[192] Because consumers face great difficulty in establishing the exact likelihood of future injury following a data breach,[193] the FTC's sliding-scale approach appears to favor consumers when the potential injury is severe.

Second, the Commissioners recognized that, in certain circumstances, subjective or emotional consumer harms may satisfy the "substantial injury"

---

183 *See* Initial Decision at 92, LabMD, Inc., No. C-9357, (F.T.C. Nov. 12, 2015), *overruled by* LabMD, Inc. v. FTC, 894 F.3d 1221 (11th Cir. 2018).

184 *See id.* at 90–92.

185 *Id.* at 54.

186 *Id.* at 14.

187 *See* Press Release, Fed. Trade Comm'n, Commission Finds LabMD Liable for Unfair Data Security Practices (July 29, 2016), https://www.ftc.gov/news-events/press-releases/2016/07/commission-finds-labmd-liable-unfair-data-security-practices; *see also* LabMD Final Order, *supra* note 164.

188 *See* LabMD Commission Opinion, *supra* note 167.

189 *Id.* at 10.

190 *Id.* at 21 ("Unlike the ALJ, we agree with Complaint Counsel that showing a 'significant risk' of injury satisfies the 'likely to cause' standard.").

191 *Id.* at 10.

192 *Id.* at 21 ("[A] practice may be unfair if the magnitude of the potential injury is large, even if the likelihood of the injury occurring is low.").

193 *See, e.g.*, Solove & Citron, *supra* note 10, at 739 ("More often than not, a plaintiff's increased risk of financial injury and anxiety is deemed insufficient to warrant recognition of harm.").

requirement, and therefore provide the basis for an unfairness claim.[194] As a result of the LabMD breach, sensitive consumer medical information was exposed to the public.[195] This included laboratory results for HIV, herpes, and prostate cancer testing.[196] While the FTC knew of only one instance in which this medical information was viewed by a third party, it concluded that consumers' attendant emotional and reputational harms were "real and substantial and thus cognizable under Section 5(n)."[197] Although the opinion limited its recognition of actual emotional injuries to breaches involving sensitive medical data,[198] this recognition is particularly significant when compared to the federal judiciary's near-outright rejection of subjective consumer data breach harms.[199]

Federal courts routinely dismiss consumer-led data security claims, highlighting the judiciary's reluctance to appreciate the many ways in which a data breach may negatively impact the consumer.[200] As a consequence, private remedies have thus far failed to provide an adequate means of post-data breach consumer redress.[201] Yet recent FTC enforcement has demonstrated a flexible approach to recognizing these very harms,[202] and as a result, stands to fill the remedial vacuum left by the courts.[203] Even before identity theft or financial fraud occurs, the Commission may be satisfied that the severity of potential consumer harm is sufficient to support a data security unfairness claim.[204] Moreover, the FTC will recognize actionable, subjective injuries when sensitive

---

194 *See* LabMD Commission Opinion, *supra* note 167, at 10 ("[I]n extreme cases, subjective types of harm might well be considered as the basis for a finding of unfairness."). *But see* Policy Statement on Unfairness, *supra* note 83 ("Emotional impact and other more subjective types of harm … will not ordinarily make a practice unfair.").

195 LabMD Commission Opinion, *supra* note 167, at 3.

196 *See id.* at 17.

197 *Id.*

198 *Id.* at 19 ("We therefore conclude that the privacy harm resulting from the unauthorized disclosure of sensitive health or medical information is in and of itself a substantial injury under Section 5(n).").

199 *See, e.g.*, Solove & Citron, *supra* note 10, at 753 ("Plaintiffs have argued that data breaches caused them emotional distress (in particular, anxiety), but courts have rejected these claims nearly every time."); *see also, e.g.*, *In re* Barnes & Noble Pin Pad Litig., No. 12–cv–8617, 2013 WL 4759588, at *5 (N.D. Ill. Sept. 3, 2013) ("Emotional distress in the wake of a security breach is insufficient to establish standing.").

200 *Supra* note 171 and accompanying text.

201 *See, e.g.*, Solove & Citron, *supra* note 10, at 754 ("[C]ases are dismissed for lack of harm even when a company's negligence has clearly caused a data breach. Even in the face of wrongful conduct by defendants, courts are denying plaintiffs redress.").

202 *See, e.g.*, Hartzog & Solove, *supra* note 10, at 2233–34 ("The FTC can regulate with a much different and more flexible understanding of harm than those focused on monetary or physical injury.").

203 *But see id.* at 2294 ("[C]ompensatory remedies are better handled by tort law or other statutes because the FTC's role is largely to discourage bad behavior, not to compensate affected parties.").

204 *See* LabMD Commission Opinion, *supra* note 167, at 21 ("[A] practice may be unfair if the magnitude of the potential injury is large, even if the likelihood of the injury occurring is low.").

medical information is implicated in a breach.[205] This responsive conception of data breach harms, in combination with the Commission's authority to obtain financial redress on behalf of consumers,[206] suggests that the FTC is uniquely situated to bring enforcement actions that meaningfully compensate affected consumers.

Therefore, the FTC's newly articulated conception of substantial injury represents a critical step in further developing the contours of a lawful data security program, and ought to be used by the Commission in any of the modes of regulation it chooses to proceed with. In any data protection unfairness action, be it an enforcement or rulemaking proceeding, the FTC must prove that the data security program in question "causes or is likely to cause substantial injury to consumers."[207] And because consumers have few viable routes to judicial redress following a data breach,[208] the FTC's flexible conception of injury stands to broaden its enforcement efforts and provide consumers with greater protection.

B. LabMD at the Eleventh Circuit: The Virtues of Specificity

Following its decision against LabMD, the FTC entered a final order against the medical testing company.[209] The order required a number of remedial measures from LabMD, including the imposition of a "comprehensive information security program" as outlined by the FTC.[210] LabMD responded by filing for judicial review in the Eleventh Circuit.[211] In its ensuing decision, the court vacated the order on the narrow grounds that the mandated security overhaul lacked the specificity required to enforce it.[212] Although *LabMD* represents an embarrassing rebuke of the FTC and its vaguely-worded

---

[205] *See id.* at 19 ("We therefore conclude that the privacy harm resulting from the unauthorized disclosure of sensitive health or medical information is in and of itself a substantial injury under Section 5(n).").

[206] *See* 15 U.S.C. § 57b(a)–(b) (2012) (describing that in an enforcement proceeding alleging that a regulated entity violated either a trade regulation rule or a final cease and desist order, the FTC Act grants the corresponding court "jurisdiction to grant such relief as the court finds necessary to redress injury to consumers").

[207] *See* 15 U.S.C. § 45(n) (2012).

[208] *See* Hartzog & Solove, *supra* note 10, at 2277 ("Contract law and tort law have not often been successfully applied to many of the issues involving the collection, storage, use, and disclosure of personal data—when courts have applied contract and tort theories to these issues, they have struggled significantly in the application.").

[209] *See* LabMD Final Order, *supra* note 164.

[210] *Id.* at 2–3.

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

[212] *See id.* at 1237 (vacating the FTC's final order for failure to "direct LabMD to cease committing an unfair practice within the meaning of Section 5(a)").

comprehensive data security overhauls, the decision did not reach the question of whether LabMD's data security program constituted an unfair practice.[213] Nonetheless, the decision strongly suggests that, in the future, the FTC must do something different.

LabMD appealed the Commission's decision under two theories.[214] First, and relevant to the above discussion on data breach harms, LabMD argued that its data security failures did not constitute an unfair act or practice under Section 5(a).[215] The Eleventh Circuit essentially punted the issue and "assume[d] *arguendo* that the Commission [was] correct and that LabMD's negligent failure[s] … constituted an unfair act or practice."[216] But because the court did not disturb the merits of the unfairness claim, the FTC should continue to use its newly articulated conception of substantial consumer injury in the data security context. And while the Commission's substantial injury standard may once again be challenged in court, *LabMD* in no way compels the FTC to alter its understanding of data breach harms. Therefore, when undertaking any future data security regulatory action, be it rulemaking or enforcement proceeding, the FTC should continue to rely on its flexible understanding of substantial consumer injury.[217]

Under the second theory, LabMD petitioned the court to rule on the enforceability of the FTC's final order. [218] The court focused on the mandated data security overhaul, which required LabMD to designate an employee to oversee its data security program, conduct a risk assessment, and design and implement "reasonable safeguards to control the risks identified through risk assessment."[219] The mandated overhaul was to last twenty years and required LabMD to retain a third-party auditor to periodically report to the FTC on compliance.[220] The Eleventh Circuit vacated the order and held that the FTC's mandated data security program was unenforceable because it did not "enjoin a specific act or practice" and said "precious little" on how the mandated program

---

213 *See id.* at 1231 ("We will assume *arguendo* that the Commission is correct and that LabMD's negligent failure to design and maintain a reasonable data-security program invaded consumers' right of privacy and thus constituted an unfair act or practice.").

214 *See id.* at 1230–31.

215 *See id.*

216 *Id.* at 1231.

217 *See supra* Part II.A.

218 *See LabMD, Inc.*, 894 F.3d at 1231.

219 LabMD Final Order, *supra* note 164, at 2–3.

220 *See id.* at 3, 6. For an extended discussion on the FTC's privacy audits, see Megan Gray, *Understanding and Improving Privacy "Audits" Under FTC Orders*, STAN. L. SCH. CTR. FOR INTERNET & SOCIETY (Apr. 18, 2018), https://cyberlaw.stanford.edu/blog/2018/04/understanding-improving-privacy-audits-under-ftc-orders.

could be implemented.[221] The text of the final order offered "an indeterminable standard of reasonableness" that LabMD could not be expected to achieve absent explicit prohibitions.[222] According to the court's reasoning, if it were to rule otherwise, it would place federal district courts in the position of managing LabMD's business obligations, a result Congress could not have envisioned.[223]

Beyond the vacated order, the long-term implications of the decision remain to be seen. The Eleventh Circuit made clear that if the Commission intends to continue imposing mandated data security overhauls, it must enjoin specific acts or practices that it deems to be unfair.[224] And this directive is consequential for the Commission. The FTC concludes the vast majority of its data security enforcement actions through negotiated settlement.[225] The documents accompanying these settlements, known as consent orders, frequently impose mandated data security overhauls closely resembling the one at issue in *LabMD*.[226]

At the time of this writing, the FTC has settled a handful of post-LabMD data security enforcement actions on the basis of its unfairness authority.[227] Having peered into its crystal ball, the Commission is confident that its complaints and consent orders contain "major changes that improve data security practices and provide greater deterrence, within the bounds of our existing authority."[228] While the attendant complaints and consent orders do

---

[221] *LabMD, Inc.*, 894 F.3d at 1237.

[222] *Id.* at 1236.

[223] *See id.* at 1237 ("The practical effect of repeatedly modifying the injunction at show cause hearings is that the district court is put in the position of managing LabMD's business in accordance with the Commission's wishes. It would be as if the Commission was LabMD's chief executive officer and the court was its operating officer. It is self-evident that this micromanaging is beyond the scope of court oversight contemplated by injunction law.").

[224] *See id.* ("[T]he Commission's cease and desist order is … unenforceable. It does not enjoin a specific act or practice.").

[225] Pardau & Edwards, *supra* note 160, at 243 (noting that "most of the [data security] cases where the FTC has pressed an unfairness argument have settled").

[226] *See, e.g.*, Final Consent Order at 3, Fandango, LLC, No. C-4481 (F.T.C. Aug. 13, 2014) (Fandango must "establish and implement, and thereafter maintain, a comprehensive security program that is reasonably designed to (1) address security risks related to the development and management of new and existing products and services for consumers, and (2) protect the security, integrity and confidentiality of covered information, whether collected by respondent or input into, stored on, captured with, or accessed through a computer using respondent's products or services").

[227] *See* Consent Order, Clixsense.com, No. C-4678 (F.T.C. June 19, 2019); FTC v. D-Link Systems, Inc., No. 3:17-cv-00039-JD (N.D. Calif. July 2, 2019); FTC v. Equifax, Inc., No. 1:19-cv-03297-TWT (N.D. Ga. July 23, 2019); Consent Order, Lightyear Dealer Technologies LLC, No. C-4687 (F.T.C. Sept. 3, 2019); Consent Order, Infotrax Systems, L.C., No. C-4696 (F.T.C. Dec. 30, 2019).

[228] *New and Improved FTC Data Security Orders: Better Guidance for Companies, Better Protection for Consumers*, FED. TRADE COMMISSION (Jan. 2020), https://www.ftc.gov/news-events/blogs/business-blog/2020/

contain an additional scintilla of specificity,[229] the Commission's claim amounts to premature self-promotion. Although no enforcement subject has sought to challenge a consent order in federal court, it would not be unreasonable to assume that one may test the waters and do so in the near future. And even if the enforceability of such orders is in fact secure, the FTC's claim of "improve[d] data security practices" and "greater deterrence" is, at best, an untested prophecy.[230]

Yet there are additional tools "within the bounds of [the FTC's] existing authority"[231] that the Commission would be well-advised to invoke. Rather than specifying the exact unfair data security practices each time it files an order, the FTC could promulgate a regulatory rule that outlines a uniform standard by which all covered data security programs are to be evaluated.[232] The final Part of this Comment will make the case for such a route, and advocate steps for its actualization.

III. THE PATH FORWARD: A RETURN TO MAGNUSON-MOSS RULEMAKING

The FTC stands at a proverbial data security crossroads. The Commission's regulatory authority in the domain of data security appears well-settled.[233] Yet the Eleventh Circuit's decision in *LabMD*[234] will almost certainly force the FTC to reconsider its approach to enforcing unfair data security practices. Therefore, the FTC must take a decisive step before it concludes its next data protection case. All five of the current FTC Commissioners are new to the job, having been sworn in between May and September of 2018.[235] As issues of information security continue to dominate headlines, it is reasonable to assume that the new commissioners will want to stake their claim and assert FTC know-how into the

---

01/new-improved-ftc-data-security-orders-better-guidance.

229 *Compare, e.g.*, Consent Order at 3-4, Clixsense.com, No. C-4678 (F.T.C. June 19, 2019), *with* Consent Order, Snapchat, Inc., No. C-4501 (F.T.C. Dec. 23, 2014).

230 *New and Improved FTC Data Security Orders: Better Guidance for Companies, Better Protection for Consumers*, FED. TRADE COMMISSION (Jan. 2020), https://www.ftc.gov/news-events/blogs/business-blog/2020/01/new-improved-ftc-data-security-orders-better-guidance.

231 *Id.*

232 *See supra* Part I.B.2.

233 Judge Salas of the District of New Jersey explicitly rejected Wyndham's contention that "the FTC does not have the authority to bring an unfairness claim involving data security." FTC v. Wyndham Worldwide Corp., 10 F. Supp. 3d 602, 607 (D.N.J. 2014). The district court's decision was subsequently affirmed by the Third Circuit. *See* FTC v. Wyndham Worldwide Corp., 799 F.3d 236, 240, 259 ("We thus affirm the District Court's decision" that "the FTC has authority to regulate cybersecurity under the unfairness prong" of Section 5).

234 894 F.3d 1221 (11th Cir. 2018).

235 *See Commissioners*, FED. TRADE COMMISSION, https://www.ftc.gov/about-ftc/commissioners (last visited Oct. 11, 2018) (providing a list of when all the current Commissioners were sworn in).

future of data protection regulation. Moreover, the prospect of federal data security legislation remains uncertain.[236] Although the political parties share a common goal, they have failed to translate their conflicting data security priorities into law,[237] suggesting that the FTC holds an institutional advantage over the legislative branch.[238] While several of the numerous proposed bills seek to empower the FTC with greater authority to regulate data security,[239] the FTC cannot simply wait on Congress to act. It needs to take action.

The FTC should resurrect its Magnuson-Moss hybrid rulemaking authority and set out on an ambitious process to specify the contours of reasonable data security. Although some of the Commission's past attempts at hybrid rulemaking took an unreasonable amount of time to complete,[240] there are reasons to believe that the FTC is capable of promulgating a data security rule expeditiously. Despite the effort it will take, the structural advantages of a shift to rulemaking will enable the FTC to craft a workable data security standard that represents industry consensus.

Part III.A will begin by explaining *why* the FTC should rein in its tendency to make policy through adjudication and settlement, and instead promulgate a data security trade regulation rule. Armed with a well-crafted and focused regulatory standard, the FTC can provide enhanced legal clarity to a regulated community actively participating in the policymaking process. Consumers also stand to benefit from a shift to hybrid rulemaking. The FTC can enforce specific prohibited practices identified by the data security rule and seek compensation for injured consumers directly in federal district court. And the Commission is well prepared to do this: Having policed data security for nearly two decades, the United States' de facto privacy regulator has developed a line of jurisprudence unrivaled on the federal level. Similarly, the FTC already has experience crafting data security rules. While these rules were specially authorized by Congress and narrowly tailored to address data security within

---

[236] *See* Tim Starks, *Everything That Didn't Happen on Cybersecurity in Congress Last Year*, POLITICO (Jan. 3, 2018), https://www.politico.com/newsletters/morning-cybersecurity/2018/01/03/everything-that-didnt-happen-on-cybersecurity-in-congress-last-year-063450 ("[L]awmakers haven't notched any significant progress on any of their top digital agenda items.").

[237] *See* Gross, *supra* note 48.

[238] *Cf.* Terry M. Moe & Scott A. Wilson, *Presidents and the Politics of Structure*, 57 L. & CONTEMP. PROBS. 1, 24–26 (1994) (arguing that the structural constraints of Congress give the executive branch an institutional advantage).

[239] *See, e.g.*, Consumer Privacy Protection Act, S. 2124, 115th Cong. (2017); Personal Data Notification and Protection Act, H.R. 3806, 115th Cong. (2017).

[240] For example, the Used Motor Vehicle Trade Regulation Rule took nine years to promulgate, and the Funeral Industry Practices Rule took roughly seven years. *See* Jeffrey S. Lubbers, *It's Time To Remove the 'Mossified' Procedures for Removing FTC Rulemaking*, 83 GEO. WASH. L. REV. 1979, 1988 (2015).

specific industries, they have laid the foundation for a broadly applicable data security rule.

Part III.B will examine *how* the FTC can formulate a rule that will survive judicial review. To do so, the FTC must resourcefully comply with Magnuson-Moss rulemaking procedure and take full advantage of the time-saving mechanisms supplied by Congress. The FTC must identify the boundaries of unfair data security with legally sufficient specificity and consider the proposed federal rule alongside comparable state data security statutes and regulations. Should the Commission give heed to these considerations, it can confidently presume that its final data security rule will survive judicial scrutiny. And once implemented, a data security rule will enable the FTC to more effectively regulate unlawful data protection practices, and in the process provide consumers with greater protection from the growing threats posed by digital harms.

A. Why the FTC Should Promulgate a Magnuson-Moss Data Security Rule

As a means of administrative policymaking, federal agencies enjoy the prerogative to choose between adjudication and rulemaking.[241] Thus, until Congress indicates otherwise, the FTC is well within its discretion to continue setting data security policy under its current adjudicatory model.[242] Yet the same discretion also enables the FTC to establish data security policy standards via Magnuson-Moss hybrid rulemaking. In *Chenery II*, the Supreme Court justified agency flexibility by highlighting circumstances in which an agency's preference for one policymaking model may better suit its administrative priorities.[243] Most germane to the FTC's current track, the Court noted that case-by-case adjudication may be most appropriate when an "agency may not have had sufficient experience with a particular problem to warrant rigidifying its tentative judgment into a hard and fast rule."[244] At the dawn of its regulatory presence in data security, the FTC was right to favor an adjudicatory model. In

---

[241] *See, e.g.*, NLRB v. Bell Aerospace Co., 416 U.S. 267, 294 (1974) ("[T]he choice between rulemaking and adjudication lies in the first instance within the [National Labor Relations] Board's discretion."); SEC v. Chenery Corp. (*Chenery II*), 332 U.S. 194, 203 (1947) ("[T]he choice made between proceeding by general rule or by individual, ad hoc litigation is one that lies primarily in the informed discretion of the administrative agency.");

[242] *See* Nat'l Petroleum Refiners Ass'n v. FTC, 482 F. 2d 672, 683 (DC Cir. 1973) ("*Chenery* … and *Bell Aerospace* cannot be ignored, for they indisputably flesh out the contemporary framework in which both the FTC and this court operate and which we must recognize.").

[243] *Chenery II*, 332 U.S. at 202–03.

[244] *Id.* at 202.

such a novel and highly technical field, it risked rigidifying a rule that could prove obsolete in the face of technological innovation.[245]

While ad hoc adjudication and settlement were appropriate during the FTC's initial foray into data security, the landscape has changed. The FTC has dealt extensively with data security, compiling an impressive body of experience in the field.[246] And although the FTC has claimed that information technology is moving too quickly to effectively codify data security standards,[247] contemporary FTC data security complaints do not look all that different than those issued a decade or more ago.[248] Because many of the same data security inadequacies are still relevant today, the notion that a data security rule would be inoperative upon promulgation is being called into question.[249] But should radically new data security principles come to light, the FTC can amend its rule to adapt to new technologies.[250] As the dangers of inadequate data security remain pervasive, regulated entities will continue seeking definite guidance on how to secure consumer data.[251] And in a climate of uncertain data security litigation, individual consumers are left with few avenues to obtain redress.[252] Today, the advantages of a data security rule outweigh yesterday's drawbacks, and suggest that both consumers and the regulated public would benefit from an altered course.[253]

---

[245] *See generally id.*

[246] Pardau & Edwards, *supra* note 160.

[247] *See* Pl.'s Resp. in Opp'n to Wyndham Hotels and Resorts' Mot. to Dismiss at 7 2:12-cv-01365, ECF No. 45, FTC v. Wyndham Worldwide Corp. (D. Ariz. Aug. 9, 2012) ("Data security industry standards are continually changing in response to evolving threats and new vulnerabilities and, as such, are 'so specialized and varying in nature as to be impossible of capture within the boundaries of a general rule.'" (quoting *Chenery II*, 332 U.S. at 202)).

[248] *See* Stegmaier & Bartnick, *supra* note 51, at 713 n.213.

[249] *See id.* at 713 ("[T]he idea that [data security] regulations would be impractical or out of date as soon they are published is not reflected by the facts.").

[250] *See* 15 U.S.C. § 57a(d)(2)(B) (2012) ("A substantive amendment to … a rule promulgated under [this] subsection … shall be prescribed … in the same manner as a rule prescribed under such subsection.").

[251] *See supra* note 121.

[252] *See supra* note 171 and accompanying text.

[253] In the field of competition, FTC Commissioner Rohit Chopra recently advocated for a shift away from adjudication and toward rulemaking as a means of policymaking. *SeeFed. Trade Comm'n, Hearing #1 on Competition and Consumer Protection in the 21st Century Before the Fed. Trade Comm'n* 7 (2018) (statement of Rohit Chopra, Comm'r) ("I see three major benefits to the FTC engaging in rulemaking under 'unfair methods of competition,' … [T]he current approach generates ambiguity, is unduly burdensome, and suffers from a democratic participation deficit. Rulemaking can create value for the marketplace and benefit the public on all of these fronts."). Although Commissioner Chopra's remarks are clearly limited to the FTC's antitrust efforts, his reasoning could be effortlessly applied to the data security context, and indicate that the FTC is, at the very least, having the relevant conversation.

Yet the FTC must contend with the heightened procedural requirements of Magnuson-Moss rulemaking, which the common narrative[254] derides as "prohibitively profligate"[255] and "procedurally burdensome."[256] Critics assert that the process has encumbered the FTC by unreasonably elongating the timeframe from rule conception to promulgation.[257] And while many of these rulemaking proceedings took an excessive amount of time to complete in the past,[258] there are reasons to believe that the FTC is capable of promulgating a data security rule in a reasonable amount of time. For example, many of the previous TRRs dealt with relatively low-priority issues,[259] such as unfair and deceptive practices in the funeral and vocational school industries.[260]

In contrast, the contemporary climate in which a data security TRR would be promulgated appears to differ from earlier, untimely FTC rulemaking efforts. A comprehensive data security rule would presumably command greater external visibility, and thus greater internal priority at the FTC. In this sense, heightened attention around data security should incentivize the FTC to conduct rulemaking in a comparatively expeditious manner.[261] Beyond contextual factors, which are admittedly difficult to verify, there are procedural considerations suggesting that the FTC is capable of completing a Magnuson-

---

[254] *See* Lubbers, *supra* note 236, at 1997–98 (arguing that Magnuson-Moss rulemaking procedures alone have contributed to the FTC's increased delay in promulgating rules).

[255] Cooper J. Spinelli, *Far from Fair, Farther from Efficient: The FTC and the Hyper-Formalization of Informal Rulemaking*, 6 LEG. & POL'Y BRIEF 129, 134 (2014),

[256] Hartzog & Solove, *supra* note 10, at 2258 n.160.

[257] *See, e.g.*, Charles H. Koch, Jr. & Beth Martin, *FTC Rulemaking Through Negotiation*, 61 N.C. L. REV. 275, 290 (1983) ("Delay … is a significant problem in the promulgation of trade regulation rules … The major cause may be no single factor or set of factors but rather the added spirit of adversarial confrontation inherent in hybrid rulemaking."); Kent Barnett, *Looking More Closely at the Platypus of Formal Rulemaking*, REG. REV. (May 11, 2017), https://www.theregreview.org/2017/05/11/barnett-platypus-formal-rulemaking ("[T]he additional procedure [of Magnuson-Moss hybrid rulemaking] may have simply allowed affected industries more time to pressure agency members—perhaps through congressional allies—into slowing down, watering down, or forgoing rulemaking.").

[258] *See* Lubbers, s*upra* note 236 and accompanying text. But the FTC has also shown that it is capable of promulgating a valid TRR in under two years. *See id.* at 1987 (noting that the FTC's Labeling and Advertising of Home Insulation rule took 1.77 years to complete, and the Ophthalmic Practice rule took 2.5 years).

[259] *See* Barnett, *supra* note 253 ("The FTC … may simply have given … the [Trade Regulation] rules low priority.").

[260] *See* Funeral Industry Practices, 40 Fed. Reg. 39,901 (proposed Aug. 29, 1975) (codified at 16 C.F.R. pt. 453); Funeral Industry Practices, 47 Fed. Reg. 42,260 (Sept. 24, 1982) (codified at 16 C.F.R. pt. 453); Advertising, Disclosure, Cooling Off and Refund Requirements Concerning Proprietary Vocational and Home Study Schools, 39 Fed. Reg. 29,385 (proposed Aug. 15, 1974) (codified at 16 C.F.R. pt. 438); Proprietary Vocational and Home Study Schools, 43 Fed. Reg. 60,796 (Dec. 28, 1978) (codified at 16 C.F.R. pt. 438).

[261] It must also be noted that heightened attention may provoke the opposite effect: a greater number of interested parties vying to participate in the rulemaking process. But, as will be argued below, the FTC can judiciously utilize its time-saving discretion to mitigate inappropriate and unnecessary delay. *See* 15 U.S.C. § 57a(c)(3) (2012).

Moss rulemaking proceeding in a reasonable amount of time. These considerations will be fully explored below in Part III.B.1.

In today's context of data security, the FTC would be well-advised to invoke its congressionally delegated rulemaking authority and codify the parameters of lawful data security. Three consequential benefits will flow from a shift to hybrid rulemaking. Broadly speaking, a data security unfairness rule can provide the FTC with (1) a democratically constructed and higher quality data security standard; (2) a more efficient use of administrative resources; and (3) a remedial capacity better suited to protecting consumers. Because the Commission has relevant experience policing data security and crafting congressionally authorized data-related rules, it is well prepared to oversee a successful hybrid rulemaking process.

First, as a general matter, policy creation through rulemaking "yields higher quality policy decisions," as it provides for public participation in the process.[262] Rulemaking would enable the FTC to establish its data security policy through transparent and democratic means, giving those who may be affected by it the chance to make their voices heard.[263] This process is far more participatory than the FTC's current adjudicatory model, in which nonparties to a dispute are unable to weigh in on the potentially altered regulation.[264]

The tech industry, the judiciary, and the public have all made it clear that they want greater specificity as to what constitutes an unlawful data security program.[265] As the leading federal data security regulatory body, the FTC is

---

[262] *See, e.g.*, Richard J. Pierce, *Two Problems in Administrative Law: Political Polarity on the District of Columbia Circuit and Judicial Deterrence of Agency Rulemaking*, 1988 DUKE L. J. 300, 308–09 ("Rulemaking yields higher quality policy decisions than adjudication because it invites broad participation in the policymaking process by all affected entities and groups, and because it encourages the agency to focus on the broad effects of its policy rather than the often idiosyncratic adjudicative facts of a specific dispute."); *see also* NLRB v. Bell Aerospace Co., 416 U.S. 267, 295 (1974) (rulemaking provides a "forum for soliciting the informed views of those affected in industry … before embarking on a new course").

[263] *See* Stegmaier & Bartnick, *supra* note 51, at 710 ("When the FTC uses its rulemaking authority, entities clearly indicate their desire to participate in rulemaking proceedings by submitting comments. Not only are entities heard, but the FTC also uses the information it receives to formulate regulations.").

[264] *See* Brice McAdoo Clagett, *Informal Action–Adjudication–Rulemaking: Some Recent Developments in Federal Administrative Law*, 1971 DUKE L.J. 51, 83 (discussing the lack of safeguards for "nonparties to [an] adjudication who may be significantly affected by the new policy").

[265] *See, e.g.*, LabMD Inc. v. FTC, 894 F.3d 1221, 1237 (11th Cir. 2018); Press Release, Internet Ass'n, Internet Association Proposes Privacy Principles for a Modern National Regulatory Framework (Sept. 12, 2018), https://internetassociation.org/internet-association-proposes-privacy-principles-for-a-modern-national-regulatory-framework; Kari Paul, *Here's the No. 1 Thing Customers Would Like Companies To Do Better*, MKT. WATCH (Nov. 14, 2018), https://www.marketwatch.com/story/heres-the-no-1-reason-people-dislike-us-companies-2018-11-13 (noting that "[d]ata privacy is the No. 1 issue people want companies to address today"). The Internet Association represents "leading global internet companies" including Amazon, eBay, PayPal and

primed to offer just that. To be sure, the FTC's current approach to enforcement provides regulated entities with legally adequate notice.[266] But the FTC should strive to provide notice that goes beyond baseline legal requirements and work together with industry to put forward a viable data security rule.

Despite its frequent castigation, Magnuson-Moss rulemaking offers the perfect venue for tackling this hot-button issue, as public participation is one of the defining features of Magnuson-Moss procedure.[267] The multilayered procedural requirements that provoke outside criticism[268] are the very means by which a sustainable framework can be codified. And while a successful rulemaking endeavor will demand agency time and resources, the process can be justified when considering both congressional inaction in passing data security legislation[269] and judicial reluctance to accept consumer data breach claims.[270] When Congress endowed the FTC with hybrid rulemaking authority, it intended the agency to deliberate with the public before promulgating specific unfairness rules.[271] Such democratic participation should not be viewed as a strain on FTC authority; rather, it should be seen as a mechanism by which good policy can be attained.

Second, successful rulemaking stands to provide the FTC with a more efficient use of administrative resources.[272] Rulemaking allows for the resolution of persistent data security regulatory issues in a singular action, as opposed to the many proceedings required under the adjudicatory model.[273] In

---

Microsoft, among others. *See Our Members*, INTERNET ALLIANCE, https://internetassociation.org/our-members/ (last visited Nov. 17, 2018).

[266] *See* FTC v. Wyndham Worldwide Corp., 799 F.3d 236, 255–56 (3d Cir. 2015) (rejecting Wyndham's argument that "it lacked notice of what *specific* cybersecurity practices are necessary to avoid liability" and holding that "[f]air notice is satisfied … as long as the company can reasonably foresee that a court could construe its conduct as falling within the meaning of" Section 5).

[267] *See, e.g.*, Ronald Marshall Rosengarten, *The Scope of Federal Trade Commission Rulemaking:* Katharine Gibbs School v. FTC, 16 NEW ENG. L. REV. 917, 918 (1980) (noting that the Magnuson-Moss Act required that "the public have generous input into the rulemaking process").

[268] *See* Lubbers, *supra* note 236.

[269] *See, e.g.*, Starks, *supra* note 232 ("[L]awmakers haven't notched any significant progress on any of their top digital agenda items.").

[270] *Supra* note 171 and accompanying text.

[271] *See* HOOFNAGLE, *supra* note 59, at 55 (noting that in passing the Magnuson-Moss Warranty–Federal Trade Commission Improvements Act, Congress required that the FTC "provide more opportunities for public participation" in rulemaking).

[272] *See, e.g.*, Nat'l Petroleum Refiners Ass'n v. FTC, 482 F.2d 672, 690 (D.C. Cir. 1973) ("There is little disagreement that the Commission will be able to proceed more expeditiously, give greater certainty to businesses subject to the Act, and deploy its internal resources more efficiently with a mixed system of rule-making and adjudication than with adjudication alone.").

[273] *See* STRAUSS ET AL., *supra* note 121, at 420 ("One powerful attraction of rulemaking is that it may permit the agency to resolve recurring regulatory issues in a single proceeding.").

addition, determining whether an entity is acting lawfully becomes less costly, as the Commission can evaluate its compliance according to the data security standard.[274] It is true that the FTC has largely avoided adjudicatory confrontations by frequently entering into settlement orders with accused Section 5 violators.[275] However, the Eleventh Circuit's rebuke in *LabMD* suggests that accused parties may be more willing to challenge FTC allegations in the future. No doubt, creating a data security rule will necessitate a serious expenditure of Commission resources.[276] Yet, in the long run, such a rule can reduce the costs of both agency enforcement and industry compliance.[277]

Third, a data security TRR will enhance the FTC's remedial capacity to protect consumers from, and compensate them for, data breach harms. From an *ex ante* perspective, a data security TRR will offer regulated entities a clearer roadmap to adequately safeguard the consumer data that they hold. With a more focused standard, the FTC's new TRR can help companies bolster their own security programs and prevent some data breaches from ever occurring.

From an *ex post* perspective, the promulgation of a data security TRR will fortify the Commission's ability to levy civil penalties against Section 5 violators. Under its current framework, the FTC can only extract monetary damages from companies that violate a previously issued FTC order.[278] Thus, only repeat offenders are forced to incur financial burdens, weakening the FTC's deterrent effect.[279] But under its Magnuson-Moss authority, the FTC can initiate a suit against an entity that commits an unfair or deceptive practice as defined by the TRR.[280] Specifically, the FTC Act gives the corresponding court "jurisdiction to grant such relief as the court finds necessary to redress injury to consumers … from the rule violation."[281] Therefore, in promulgating a

---

[274] *See* Stegmaier & Bartnick, *supra* note 51, at 712 (arguing that FTC rulemaking constitutes a more efficient use of resources, in part because "determining whether a regulated entity is noncompliant is much easier, because the agency has a clear standard to apply to the entities' behavior").

[275] *See* Pardau & Edwards, *supra* note 160.

[276] *See* Colin S. Diver, *The Optimal Precision of Administrative Rules*, 93 YALE L.J. 65, 73–74 (1983) (discussing the costs associated with rulemaking).

[277] *See* Stegmaier, *supra* note 51, at 712 ("[T]here are potentially significant cost savings after [a] regulation becomes law. First, when a regulation is clear, voluntary compliance is more likely because compliance is easier to determine. Second, determining whether a regulated entity is noncompliant is much easier, because the agency has a clear standard to apply to the entities' behavior.").

[278] *See* 15 U.S.C. § 45(l) (2012).

[279] *Cf.* Max Minzner, *Why Agencies Punish*, 53 WM. & MARY L. REV. 853, 856 (2012) ("Through their [financial] penalties, agencies seek to achieve positive social outcomes. For example, penalties might deter misconduct by raising the expected cost of violations above the cost of compliance.").

[280] *See* 15 U.S.C. § 57b(b).

[281] *Id.* The provision goes on to specify:

cybersecurity TRR, the FTC need not find that a violator has breached an order to hold it financially responsible. Instead, it can seek civil penalties as a first step remedy.

In addition, the Commission's authority to enforce its data security TRR[282] can incentivize future compliance from entities that have sustained a data breach. If the FTC settles with a TRR-violating company, rather than bringing the matter to court, it can fashion an order that points to the specific security deficiency that prompted noncompliance. From there, the Commission can mandate the flaw's correction with the degree of specificity required under *LabMD*.

Therefore, in creating a data security TRR, the FTC can further consolidate its remedial capacity to protect consumers. Such a TRR can help companies bolster their own security programs before a breach occurs. When a breach does occur, a data security TRR will facilitate *ex post* consumer redress to the very individuals who were harmed by that specific breach and provide the breached company with particularized guidance for future compliance. Because federal courts have largely rejected consumer data breach remedies,[283] a data security TRR will enable the FTC to fill the vacuum and extract consumer redress with greater administrative ease.

Rulemaking is an admittedly complex process.[284] The attentive eye of judicial review demands that agencies have an intimate knowledge of the technical substance of a proposed rule, as well as the rulemaking's procedural requirements.[285] Having regulated data security for nearly twenty years, the FTC has already established the foundation from which an unfairness data security TRR will be built on. In that sense, the Commission has already done a great deal of work in paving the way for meaningful public engagement. Through its enforcement actions and guidance documents, the FTC has established a body

---

> Such relief may include, but shall not be limited to, rescission or reformation of contracts, the refund of money or return of property, the payment of damages, and public notification respecting the rule violation or the unfair or deceptive act or practice, as the case may be; except that nothing in this subsection is intended to authorize the imposition of any exemplary or punitive damages.

Id.

[282] *See* 15 U.S.C. § 57b(a)(1); *see also* OPERATING MANUAL, *supra* note 136, § 7.3.28.2 ("Enforcement of TRR's").

[283] *Supra* note 171 and accompanying text.

[284] *See* Administrative Procedure Act, 5 U.S.C. § 553 (2012) ("Rule making"); *supra* note 138.

[285] *Cf.* Daniel J. Gifford, *Administrative Rulemaking and Judicial Review: Some Conceptual Models*, 65 MINN. L. REV. 63, 65 (1980) ("Judicial review of rules on the record of the rulemaking proceeding requires that all material relevant to assessing the validity of the rules, including 'factual' material, be found in the administrative record.").

of jurisprudence that carries serious weight.[286] This jurisprudence provides a substantive list of practices that the FTC deems to contribute to unreasonable data security. And these practices were not identified in a vacuum. The FTC has been acting as a norm codifier, looking to industry best practices as they continue to develop toward a baseline standard.[287] Moreover, the FTC has promulgated several industry-focused data-related rules pursuant to specific congressional authorization, including the GLBA Safeguard Rule,[288] the FACTA Red Flags Rule,[289] and the COPPA Rule.[290] While these rulemaking proceedings were not subject to Magnuson-Moss procedure, they nonetheless show that the FTC has a background in articulating rule-based regulatory standards in the context of information privacy.[291] The FTC can and should build on these rulemaking experiences and confidently focus their efforts on delineating a broadly applicable data security standard. And finally, the FTC can look to emerging state data security laws[292] when crafting its own related TRR. Recognizing its own informational advantage, the Commission ought to embrace states as the laboratories of democracy,[293] evaluating the successes and shortcomings of ambitious local lawmaking, and skillfully incorporating the most expedient standards and frameworks to effectively regulate data security on the federal plane.

Regardless of these considerations, an FTC data security rule will fail to launch if a reviewing court determines that it exceeds the Commission's

---

[286] *See* Solove & Hartzog, *supra* note 27.

[287] *See id.* at 636 ("The FTC has come to rely on industry standards and other norms to identify a particular set of practices that, taken together, constitute adequate security practices for companies collecting personal information.").

[288] Standards for Safeguarding Customer Information, 67 Fed. Reg. 36,484 (May 23, 2002) (codified at 16 C.F.R. pt. 314).

[289] Identity Theft Red Flags and Address Discrepancies Under the Fair and Accurate Credit Transactions Act of 2003, 72 Fed. Reg. 63,718 (Nov. 9, 2007) (codified at 16 C.F.R. pt. 681).

[290] Children's Online Privacy Protection Rule, 64 Fed. Reg. 59,888 (Nov. 3, 1999) (codified at 16 C.F.R. pt. 312).

[291] *See* Stegmaier & Bartnick, *supra* note 51, at 709 (arguing that the COPPA and FACTA rulemakings show that "the FTC has experience crafting rules and detailed guidelines related to data-related practices").

[292] For example, Ohio's newly enacted Cybersecurity Safe Harbor Act, which is among the first legislative attempts to define the contours of a reasonable cybersecurity program, tracks the standards promulgated by the Commerce Department's National Institute of Standards and Technology. *See* OHIO REV. CODE §§ 1354.02–1354.03 (West 2018); *see also, e.g.*, Standards for the Protection of Personal Information of Residents of the Commonwealth, 201 MASS. CODE REGS. 17.00 (2010); Financial Data Protection and Consumer Notification of Data Security Breach Act, NEB. REV. STAT. § 87–808 (2006) (amended in 2017); Cybersecurity Requirements for Financial Services Companies, N.Y. FIN. SERV. LAW §§ 500.03–500.16 (2017).

[293] *See* New State Ice Co. v. Liebmann, 285 U.S. 262, 311 (1932) ("It is one of the happy incidents of the federal system that a single courageous state may, if its citizens choose, serve as a laboratory; and try novel social and economic experiments without risk to the rest of the country.").

authority. The following Section will identify the most important considerations pertaining to judicial review of the rule and suggest certain priorities that the Commission ought to address when crafting it.

B. Anticipating Judicial Review: How to Formulate a Durable Data Security Rule

As with any agency-promulgated rule, an FTC data security TRR may be subject to judicial review in a federal court.[294] Affected parties are afforded the opportunity to challenge the rule under either the grounds specified in the Magnuson-Moss Act, or those included in Section 706(2) of the Administrative Procedure Act.[295] Thus, to ensure that its considerable rulemaking efforts are not in vain, the FTC must anticipate the potential arguments that may seek to invalidate the rule. At present, the FTC is entirely capable of crafting a data security rule that will pass judicial muster. But to do so, it must consider three factors related to the procedure and content of the proposed rule. First, although the Commission retains some discretion to limit access to public hearings, it must respect procedural due process rights and carefully abide by the statutory requirements of Magnuson-Moss rulemaking. Second, the FTC must define unfair data security with sufficient specificity so as to not exceed its broadly construed statutory authority. And finally, the FTC will be obligated to consider preemption with regard to state laws regulating data security. Each factor will be explored in turn.

1. Expeditiously Sticking to Procedure

The first means by which a party may seek to invalidate the proposed data security rule is a challenge to the FTC's procedural obligations under the

---

[294] *See* 15 U.S.C. § 57a(e)(1)(A) (2012) ("Not later than 60 days after a rule is promulgated under subsection (a)(1)(B) by the Commission, any interested person (including a consumer or consumer organization) may file a petition, in the United States Court of Appeals for the District of Columbia circuit or for the circuit in which such person resides or has his principal place of business, for judicial review of such rule."); *see also* 5 U.S.C. § 706(2) (2012) (describing the Administrative Procedure Act's provision on the scope of judicial review).

[295] *See* 15 U.S.C. § 57a(e)(3) ("The court shall hold unlawful and set aside the rule on any ground specified in subparagraphs (A), (B), (C), or (D) of section 706(2) of title 5 … or if- (A) the court finds that the Commission's action is not supported by substantial evidence in the rulemaking record … taken as a whole, or; (B) the court finds that- (i) a Commission determination … that the petitioner is not entitled to conduct cross-examination or make rebuttal submissions, or (ii) a Commission rule or ruling … limiting the petitioner's cross-examination or rebuttal submissions, has precluded disclosure of disputed material facts."); *see also* 5 U.S.C. § 706(2) (specifying that a court may review challenges to an agency's rule on grounds of its being: (a) arbitrary, capricious, an abuse of discretion, or otherwise not in accordance with law; (b) contrary to a constitutional right or power; (c) in excess of statutory jurisdiction or authority; or (d) without observance of required procedure).

Magnuson-Moss Act.[296] Less onerous than formal rulemaking,[297] Magnuson-Moss hybrid rulemaking imposes a number of procedural steps that go beyond the notice-and-comment rulemaking to which most agencies are subject.[298] If the FTC fails to respect Magnuson-Moss procedure, the subsequent TRR will be remanded back to the Commission as a contravention of the regulated public's statutory procedural rights.[299] Therefore, careful adherence to procedure is the FTC's first step to ensuring that its data security TRR survives past infancy.

Those who argue against the use of Magnuson-Moss rulemaking point to the unreasonable amount of time it has taken the FTC to promulgate such rules in the past.[300] In particular, opponents claim that oral testimony and cross-examination, two prominent features of hybrid FTC rulemaking, have been used as "delaying device[s] for those attempting to avoid law enforcement."[301] While critics are correct that public hearing requirements are ripe for undue manipulation, they have given scarce attention to the fact that Congress anticipated this exact issue[302] and endowed the FTC with several discretionary mechanisms specifically intended to "avoid unnecessary cost and delay" during oral and cross-examination proceedings.[303]

For example, while the Magnuson-Moss Act entitles an interested person the right "to present his position orally,"[304] the Commission may impose "reasonable time limits on each interested person's oral presentations."[305] As a

---

[296] *See* 15 U.S.C. § 57a(e)(3)(B); *see also* Harry & Bryant Co. v. FTC, 726 F.2d 993, 996 (4th Cir. 1984) (petitioner's attempt to invalidate the FTC's Funeral Industry Practices Rule by reason of its procedural deficiency was unsuccessful).

[297] *See* 5 U.S.C. §§ 556–557 (2012) (outlining the procedures required under formal rulemaking).

[298] *See, e.g.*, TODD GARVEY, CONG. RESEARCH SERV., R41546, A BRIEF OVERVIEW OF RULEMAKING AND JUDICIAL REVIEW 4 (2017) (describing how hybrid rulemaking statutes "create a rulemaking process with more flexibility than the formal rulemaking procedures under [5 U.S.C.] § 556 and § 557 and more public participation than informal rulemaking procedures under § 553").

[299] *See* 5 U.S.C. § 706(2)(D) (stating that a reviewing court shall "hold unlawful and set aside agency action … found to be … without observance of procedure required by law").

[300] Lubbers, *supra* note 236.

[301] Koch, Jr. & Martin, *supra* note 253.

[302] *See* Rosengarten, *supra* note 263, at 926 ("[T]he Senate sponsors of the [Magnuson-Moss Act] were fearful that the concessions to cross-examination might be abused by the parties testifying and would need to be reconsidered. It is significant that Congress left the Commission to use its discretion in all phases of the [hybrid rulemaking] process … All these [discretionary] decisions are ultimately reviewable by the court, yet it appears that Congress lodged considerably more trust in the FTC than the fact of review might suggest.").

[303] 15 U.S.C. § 57a(c)(3) (2012); *see also* S. REP. NO. 92-269, at 26 (1971) ("The Commission would continue the proceedings only if there was 'a disparity of views concerning material facts upon which the proposed rule is based.' It is important to note that there must be a 'disparity of views' concerning 'facts' (as opposed to questions of policy) which are 'material.'").

[304] 15 U.S.C. § 57a(c)(2)(A).

[305] § 57a(c)(3)(A); *see also* OPERATING MANUAL, *supra* note 136, § 7.3.19.3.3.1 ("[T]he Presiding Officer

general matter, the Presiding Officer (PO) is empowered to "prescribe rules or issue rulings to avoid unnecessary costs or delay."[306] In contrast with oral hearings, the right to cross-examination is only necessary if the PO "determines that there are disputed issues of material fact" which are "appropriate" and "required for a full and true disclosure" of the relevant issues.[307] The PO also retains discretion to conduct cross-examination on an interested party's behalf.[308] Finally, if the PO determines that multiple parties have "the same or similar interests in the proceeding," it may limit "the representation of such interest[s]" and govern "the manner in which such cross-examination shall be limited."[309]

Taken together, the Magnuson-Moss Act leaves the FTC with meaningful room to conduct rulemaking proceedings in a timely manner, while still living up to its procedural obligations.[310] But in utilizing these time-saving discretionary mechanisms, the Commission must balance the added value of permitting certain parties to participate in informal public hearings with the legitimate purpose of avoiding unnecessary delay.[311]

If history serves as any precedent, there is reason to believe that a reviewing court will give deference to the Commission's rulings reasonably limiting the scope and availability of oral testimony and cross-examination. In *Harry & Bryant Co. v. FTC*, the only purely procedural challenge thus far to an FTC TRR, the Fourth Circuit rejected the petitioners' allegations that the FTC impermissibly limited opportunities for oral testimony and cross-examination during the Funeral Industry Practices hybrid rulemaking process.[312] Specifically, the PO restricted the number of anti-rule witnesses,[313] denied certain petitioners

has the power to limit the number of witnesses at the hearings in the interests of an orderly conduct of the proceeding. The Presiding Officer may set maximum time limits for groups of industry and staff witnesses … [T]he Presiding Officer has the power to set reasonable time limits on each witnesses' oral presentation … [and] may exercise the power to limit the number of witnesses if a large number of individuals seek to present essentially repetitious comments, views, or arguments."); *id.* § 7.3.20 ("The responsibility for the orderly conduct of the hearings lies with the Presiding Officer, who is free to exercise discretion in fulfilling this responsibility.").

306 16 C.F.R. § 1.13(c)(2)(iv) (2018). The subsection continues: "Such rules or rulings may include, but are not limited to, the imposition of reasonable time limits on each person's oral presentation…." *Id.*

307 15 U.S.C. § 57a(c)(2)(B).

308 *See id.* § 57a(c)(3)(B)(i)–(ii).

309 *Id.* § 57a(c)(4)(A)–(B); *see also* OPERATING MANUAL, *supra* note 136, § 7.3.20.1 ("[T]he Presiding Officer has the power to set reasonable time limits on cross-examination regardless of any limits on its scope.").

310 *See* Rosengarten, *supra* note 264.

311 *See supra* notes 300–06 and accompanying text.

312 726 F.2d 993, 997 (4th Cir. 1984).

313 *See id.* ("Petitioners first allege that the Commission violated Section 18 of the [FTC] Act because the Presiding Officer limited the number of witnesses permitted to give oral testimony and allowed equal numbers

the right to cross-examine consumers,[314] and conducted consumer cross-examinations himself.[315] The court affirmed the PO's discretion to limit public access under his authority "to make rulings for the purpose of avoiding unnecessary delay."[316] Because the petitioners were not denied their procedural rights, the court affirmed the Funeral Industry Practices Rule in its entirety.[317] Yet *Harry & Bryant* only reveals so much. While a reviewing judge will defer to a PO's reasonable restriction of public hearing procedures, the decision did not delineate the outer bounds of such discretion.[318]

The FTC can also look to federal jurisprudence concerning other agencies' discretion to limit opportunities for public hearing. In *Citizens Awareness Network v. United States*, a group of anti-nuclear organizations challenged the Nuclear Regulatory Commission's (NRC) revamped interpretation of the public's procedural rights during nuclear reactor licensing hearings.[319] Specifically, the NRC narrowed the availability of cross-examination during these proceedings, a type of formal adjudication.[320] The First Circuit held that the interpretation was a lawful exercise of agency discretion under Section 556(d) of the Administrative Procedure Act.[321] The NRC's primary justification behind revising its interpretation of public access was to save time—previous hearings had taken up to seven years to complete.[322] The court focused on the need for procedural flexibility, calling it "one of the great hallmarks of the

---

of pro-rule and anti-rule witnesses to testify, even though a larger number of anti-rule witnesses had applied.").

[314] *See id.* ("[P]etitioners complain that they were denied their right to cross-examine consumers.").

[315] *See id.* at 998 ("[P]etitioners allege that the Presiding Officer erred in requiring that interested parties give him written questions for consumer witnesses, which he then used to cross-examine those witnesses himself."); *see also id.* at 997–98 ("Section 18 [of the FTC Act] does not provide an automatic right to cross-examine or rebut every comment that is made a part of the rule-making record."); *id.* at 997 ("Section 18 [of the FTC Act] does not guarantee every person a right to testify.").

[316] *Id.*

[317] *See id.* at 997–99 ("Petitioners complain that they were denied numerous procedural due-process rights during the rule-making proceeding. We find no merit in any of these challenges.").

[318] The rule at issue in *Harry & Bryant*, the Funeral Industry Practices Rule, took seven years to promulgate. *See* Lubbers, *supra* note 236, at 1988 n.65. While the FTC's efforts to limit the availability of oral testimony and cross-examination did not yield a timely rulemaking process in this particular case, there are other, unexplored factors that may have contributed to the delay. In particular, the Commission likely assigned a low level of priority to regulating the funeral industry. Therefore, assuming that the FTC assigns the creation of a data security rule a high level of administrative priority, its efficient promulgation is still feasible.

[319] Citizens Awareness Network v. United States, 391 F.3d 338 (1st Cir. 2004).

[320] *See id.* at 343.

[321] *See id.* at 354 ("[W]e find no fault with the Commission's decision to attempt to curtail unnecessary cross-examination … Accordingly, we cannot say that it is arbitrary and capricious for the Commission to leave the determination of whether cross-examination will further the truth-seeking process in a particular proceeding to the discretion of the individual hearing officer.").

[322] *See id.* at 343 (describing how nuclear reactor licensing proceedings "proved to be very lengthy; some lasted as long as seven years").

administrative process … that courts must be reluctant to curtail."[323] While the First Circuit ruled in favor of the interpretation, it did note that "the [Nuclear Regulatory] Commission's new rules may approach the outer bounds of what is permissible."[324] To be sure, the FTC's rulemaking procedures are distinguishable in that they must comport with both the Magnuson-Moss Act and the Administrative Procedure Act.[325] Nonetheless, *Citizens Awareness Network* elucidates the outer bounds of agency discretion when narrowing the opportunities for oral testimony and cross-examination, and further suggests that a reviewing court may be reluctant to overturn reasonable FTC decisions intended to avoid unnecessary delay.

The preceding analysis is not meant to suggest that the FTC has free reign to restrict legitimate public access to informal hearings. But the discretionary leeway incorporated into the Magnuson-Moss Act, in combination with likely judicial deference, does suggest that the FTC can reasonably limit the availability of oral testimony and cross-examination, while still complying with its procedural obligations. This consideration, alongside the high-profile character of data security, indicates that the FTC is capable of overseeing a comparatively swift rulemaking proceeding that can withstand judicial oversight.

2. Defining Unfair Practices with Specificity

Pursuant to Section 18 of the FTC Act, the Commission is empowered to promulgate "rules which define with specificity acts or practices which are unfair or deceptive."[326] The FTC may also include in its rule "requirements prescribed for the purpose of preventing such acts or practices."[327] If an affected party seeks to invalidate a TRR for lack of specificity, the reviewing court "must perform [its] quintessential judicial function of determining whether the Commission has acted within the bounds of its statutory authority."[328] Simultaneously, the reviewing court must give "controlling weight" to the

---

[323] *Id.* at 355; *see also id.* ("We cannot say that the Commission's desire for more expeditious adjudications is unreasonable, nor can we say that the changes embodied in the new rules are an eccentric or a plainly inadequate means for achieving the Commission's goals."); *id.* at 361 (Lipez, J., concurring) ("[F]lexibility has always been a hallmark of the APA, and … agencies have always had considerable discretion to structure on-the-record hearings to suit their particular needs. This flexibility is nowhere more evident than in determining the role of cross-examination in on-the-record hearings.").

[324] *Id.* at 355.

[325] *See* 15 U.S.C. § 57a(b)(1) (2012).

[326] *Id.* § 57a(1)(B).

[327] *Id.*

[328] Am. Fin. Servs. Ass'n v. FTC, 767 F.2d 957, 968 (D.C. Cir. 1985).

FTC's interpretation of its own statute unless it is "arbitrary, capricious, or manifestly contrary to the statute."[329]

Since Congress passed the Magnuson-Moss Act, only one FTC TRR has been invalidated for lack of specificity.[330] In *Katharine Gibbs School Inc. v. FTC*, the Second Circuit set aside the Commission's newly promulgated Vocational Schools Rule over its failure to comply with Section 18's specificity requirements.[331] In examining the text of the Vocational Schools Rule, the court found that instead of identifying a specific unfair act or practice, the Rule declared that any school failing to comply with its requirements would be engaging in an unfair act or practice.[332] For example, the Rule required covered schools to partially refund students who had dropped out before the end of the semester.[333] If the regulated school neglected to refund such a student, it would be performing an unfair practice.[334] Accordingly, the court determined that the FTC had defined unfair practices in terms of future violations of the Rule's remedial requirements.[335] Because this was contrary to Section 18, the court set aside the rule and remanded it back to the Commission.[336]

Equally as instructive, several courts have upheld the specificity of other FTC TRRs.[337] In *American Financial Services Association v. FTC*, the D.C. Circuit affirmed the validity of the FTC's Credit Practices Rule because it "identifie[d] specific practices … as *per se* unfair."[338] For example, the Credit Practices Rule contains a provision declaring that lenders and retailers cannot

---

329 Chevron, U.S.A., Inc. v. Nat. Res. Def. Council, Inc., 467 U.S. 837, 843 (1984).

330 *See* Katharine Gibbs Sch. Inc. v. FTC, 612 F.2d 658 (2d Cir. 1979).

331 *Id.* at 670.

332 *See id.* at 662 n.3 ("The Commission's Rule provides simply that it is an unfair or deceptive act or practice for any school to fail to comply with the requirements of the Rule.").

333 *See id.* at 662–63.

334 *See id.*

335 *See id.* at 662 ("Requirements designed to prevent unfair practices are predicated upon the existence of unfair practices. These unfair practices, which are the statutorily required underpinning for the Commission's 'requirements', should have been defined with specificity.").

336 *See id.* ("Instead of defining with specificity those acts or practices which it found to be unfair or deceptive, the Commission contented itself with treating violations of its 'requirements prescribed for the purpose of preventing' unfair practices as themselves the unfair practices. We think that Congress expected more than this.").

337 *See* Am. Fin. Servs. Ass'n v. FTC, 767 F.2d 957, 984 (D.C. Cir. 1984) ("The Commission having defined with specificity the acts or practices deemed unfair has fully complied with the statutory requirements of section 18(a)(1)(B)."); Harry & Bryant Co. v. FTC, 726 F.2d 993, 999 (4th Cir. 1984) ("The Funeral Rule defines unfair practices in the sale of funeral goods and services and prescribes preventative requirements. It clearly falls within the Commission's statutory authority."); United States v. Hertz Corp., No. 78-6413-Civ-JLK, 1981 WL 2075, at *3 (S.D. Fla. Apr. 29, 1981) (rejecting plaintiff's argument that the Preservation of Consumers' Claims and Defenses Rule failed to "properly … define an unfair or deceptive practice").

338 *Am. Fin. Servs.*, 767 F.2d at 984.

extend credit to consumers when that credit is predicated on an assignment of wages.[339] The provision includes "requirements prescribed for the purpose of preventing such acts"[340] by identifying three scenarios in which a lender or seller *can* accept wage assignments, without acting unfairly.[341] Distinguishing the Credit Practices Rule with the invalidated Vocational Schools Rule, the D.C. Circuit found that because "the direct relationship between the unfair practice and the proscription of that practice is apparent … there is no reason to set out the two separately."[342]

Taken together, the FTC ought to use *Katharine Gibbs* and *American Financial Services* as guideposts when drawing up a data security TRR. The FTC must first define specific data security practices that are per se unfair.[343] And only then can the Commission lay out requirements intended to prevent unfair data security programs.[344] These requirement provisions will be crucial to the workability of the proposed TRR because they will inject a degree of nuance into the TRR that reflects the evolving character of data security.

But of course, identifying specific unfair data security practices is easier said than done. FTC guidance documents routinely profess that "[t]here's no one-size-fits-all approach to data security, and what's right for you depends on the nature of the business and the kind of information you collect from your customers."[345] Yet in closely examining every FTC data security complaint, a number of recurring unfair data security practices frequently surface.[346] For example, Professors Solove and Hartzog argue that the Commission has in fact provided a substantive list of specific unfair data security practices.[347] Some of

---

339 *See* 16 C.F.R. § 444.2(a)(3) (2018) ("In connection with the extension of credit to consumers … it is an unfair act or practice … for a lender or retail installment seller … to take or receive from a consumer an obligation that … [c]onstitutes or contains an assignment of wages.").

340 15 U.S.C. § 57a(1)(B) (2012).

341 *See* 16 C.F.R. § 444.2(a)(3)(i)–(iii) (2018) (if the assignment (i) is revocable at will by the debtor; (ii) is a payment reduction plan; or (iii) applies only to wages already earned at the time of assignment).

342 *Am. Fin. Servs.*, 767 F.2d at 984 (quoting Credit Practices Rule, 49 Fed. Reg. 7740, 7745 (Mar. 1, 1984) (codified at 16 C.F.R. pt. 444)).

343 *See id.* ("The Commission having defined with specificity the acts or practices deemed unfair has fully complied with the statutory requirements of section 18(a)(1)(B)" of the FTC Act).

344 *See* Katharine Gibbs Sch. Inc. v. FTC, 612 F.2d 658, 662 (2d Cir. 1979) ("Requirements designed to prevent unfair practices are predicated upon the existence of unfair practices. These unfair practices, which are the statutorily required underpinning for the Commission's 'requirements', should have been defined with specificity.").

345 *E.g.*, FED. TRADE COMM'N, PROTECTING PERSONAL INFORMATION: A GUIDE FOR BUSINESS 31 (2016).

346 *See* Solove & Hartzog, *supra* note 27, at 650 (noting that "a detailed list of problematic security practices has emerged" from the FTC's data security complaints).

347 *Id.* at 650–51 ("[V]iewed collectively, the FTC's data security jurisprudence forms a rather detailed list of inadequate security practices.").

these unfair practices include allowing data to be vulnerable to common attacks (such as Structured Query Language injection), a lack of digital encryption, making data easily available, failure to test the security of a product or process, failure to remedy known security vulnerabilities, a lack of data minimization, failure to train employees in proper data security, poor username and password protocols, and many more.[348] When creating its data security rule, the FTC should look to its own complaints, and condense and prioritize the most pressing data security vulnerabilities. Using these particular unfair data security practices, the Commission can equip its data security rule with the requisite degree of specificity.

The FTC should also look to the HIPAA Security Rule, a data security regulatory standard promulgated and administered by the Department of Health and Human Services.[349] The Security Rule, which applies to certain entities that collect and use consumer health data, lays out a number of specific administrative, physical, and technical safeguards that covered entities must consider.[350] Many of these safeguards align with the FTC's, including requirements for a designated security official, security awareness and training for employees, log-in monitoring, password management, security incidence procedures, encryption, automatic logoff, and others.[351] Because the HIPAA Security Rule is regarded as "one of the most specific data security laws,"[352] the FTC should endeavor to craft its own data security rule in a similar manner.

In sum, specificity is critical. From the beginning of its rulemaking process, the FTC must define unfair data security acts with definite precision. The Commission may look to several sources when doing so, including its own privacy jurisprudence, as well as the specifically tailored HIPAA Security Rule and other federal data security regulatory rules. If it does so, the Commission

---

348 *See id.* at 651–55.

349 45 C.F.R. § 164.308–164.312 (2013).

350 *See id.* The HIPAA Security Rule contains implementation specifications that are either "required" or "addressable." *Id.* § 164.306(d)(1). When a standard contained within the Security Rule is "addressable," the covered entity must "[a]ssess whether each implementation specification is a reasonable and appropriate safeguard in its environment, when analyzed with reference to the likely contribution to protecting electronic protected health information." *Id.* § 164.306(d)(3)(i). If the entity determines that implementing the specification is "reasonable and appropriate," it must do so. *See id.* § 164.306(d)(3)(ii)(A). If it is not, the entity must "[d]ocument why it would not be reasonable and appropriate to implement the implementation specification." *Id.* § 164.306(d)(3)(ii)(B)(1).

351 *See id.* § 164.308(a)(2) ("Assigned security responsibility"); *id.* § 164.308(a)(5)(i) ("Security awareness and training"); *id.* § 164.308(a)(5)(ii)(C) ("Log-in monitoring"); *id.* § 164.308(a)(5)(ii)(D) ("Password management"); *id.* § 164.308(a)(6)(i)–(ii) ("Security incident procedures"); *id.* § 164.312(a)(2)(iv) ("Encryption and decryption"); *id.* § 164.312(a)(2)(iii) ("Automatic logoff").

352 Solove & Hartzog, *supra* note 27, at 655.

can avert the *Katherine Gibbs* issue and improve its chances during judicial review.

3. Preemption

The U.S. federal government is not alone in its efforts to regulate data security. In the absence of any comprehensive federal law outlining reasonable data security, several states have ambitiously waded into the arena by passing legislation or promulgating regulations on the matter.[353] Although the Magnuson-Moss Act does not contain an explicit preemption provision, legally sound FTC regulations may supersede comparable state statutes and regulations.[354] However, should the FTC put forth a novel TRR tracing the boundaries of legally adequate data security, the Commission must carefully consider its interaction with analogous state laws so as to avoid its invalidation on grounds of overbroad preemption.

Once again, *Katharine Gibbs*[355] and *American Financial Services*[356] can serve as instructive bookends that the FTC ought to use when crafting a durable data security TRR. In *Katharine Gibbs*, the Second Circuit held that the enactment of the Vocational Schools Rule's preemption provision went beyond the FTC's congressionally allocated authority because it was impermissibly overbroad.[357] Specifically, the provision stated that the Vocational Schools Rule "preempts any provision of any state law, rule, or regulation which is inconsistent with or otherwise frustrates the purpose of the provisions of this trade regulation rule."[358] Because the purpose of the Rule was stated in general terms,[359] the court sought to avoid a scenario in which any state law governing the contractual relationship between vocational schools and their students may

---

353 *See* Standards for the Protection of Personal Information of Residents of the Commonwealth, 201 MASS. CODE REGS. 17.00 (2010); Financial Data Protection and Consumer Notification of Data Security Breach Act, NEB. REV. STAT. § 87–808 (2006) (amended in 2017); Cybersecurity Requirements for Financial Services Companies, N.Y. COMP. CODES R. & REGS. tit. 23, §§ 500.03–500.16 (2017); OHIO REV. CODE ANN. §§ 1354.02–1354.03 (West 2018).

354 *See* Katharine Gibbs Sch. Inc. v. FTC, 612 F.2d 658, 667 (2d Cir. 1979) (citing Free v. Bland, 82 S. Ct. 1089 (1962) and Spiegel Inc. v. FTC, 540 F.2d 287, 293 (7th Cir. 1976)) ("It has long since been firmly established that state statutes and regulations may be superseded by validly enacted regulations of federal agencies such as the FTC.").

355 612 F.2d 658.

356 767 F.2d 957.

357 *See Katharine Gibbs*, 612 F.2d at 667.

358 16 C.F.R. § 438.9 (repealed 1979).

359 *See* Vocational Schools Rule, 43 Fed. Reg. 60,796, 60,796 (Dec. 28, 1978) (codified at 16 C.F.R. pt. 438) ("The purpose of [the Vocational Schools Rule] is to alleviate currently abusive practices against vocational and home study school students and prospective students.").

be preempted.[360] Gleaning the Magnuson-Moss Act's legislative history, the court indicated that the FTC's regulations "were to have no more preemptive effect than that which flows inevitably from a repugnancy between the Commission's valid enactments and state regulations."[361]

In contrast, *American Financial Services* saw the D.C. Circuit endorse the preemption provision contained within the FTC's Credit Practices Rule.[362] In doing so, the court pointed to three factors that distinguished the Credit Practices Rule's preemptive character from its defective Vocational Schools Rule counterpart.[363] First, the Credit Practices Rule explicitly manifested an intent not to occupy the field of credit regulation.[364] Second, the Rule's Statement of Basis and Purpose noted that the FTC considered and modified the Rule to be as consistent as possible with corresponding state laws.[365] Lastly, the Credit Practices Rule contained an exemption provision for states with comparable laws that offered equal or greater protection for consumers.[366] In combination, the court found that the FTC did not exceed its preemption authority.[367]

To the modern FTC, *Katharine Gibbs* represents the dangers associated with an overly broad preemption clause.[368] In that sense, the FTC's data security TRR should only purport to preempt state laws that are inconsistent with its particularized purposes, rather than occupying the entire field of information security. So too, *American Financial Services* offers practical steps that the FTC can replicate when considering preemption in the data security context.[369] The FTC should look to the successes and limitations of comparable state data security laws, make explicit its intent not to occupy the field, and include a

---

360 *See Katharine Gibbs*, 612 F.2d at 667.

361 *Id.*; *see also* Paul R. Verkuil, *Preemption of State Law by the Federal Trade Commission*, 25 DUKE L.J. 225, 247 (1976) ("While the Commission was not given the authority broadly to occupy the field of state unfair competition in consumer protection law, it was authorized to declare by rule preemption of state activities that conflict with federal regulations.").

362 *See* Am. Fin. Servs. Ass'n v. FTC, 767 F.2d 957, 990–91 (D.C. Cir. 1984).

363 *See id.*

364 *See* Credit Practices Rule, 49 Fed. Reg. 7740, 7783 (Mar. 1, 1984) (codified at 16 C.F.R. pt. 444) ("[T]he rule is not intended to occupy the field of credit regulation or to preempt state law in the absence of requirements that are inconsistent with the rule.").

365 *See id.* at 7782 ("The rule has been drafted to be as consistent with existing state laws as possible. Indeed, state laws served as the model for several rule provisions. The rule prohibits practices that are authorized by statute or common law in at least some states. However, none of the rule provisions *preempts* state law by creating an irreconcilable conflict. That is, creditors will be able to comply with both state law and this rule." (emphasis in original)).

366 *See* 16 C.F.R. § 444.5 (2018).

367 *See Am. Fin. Servs.*, 767 F.2d at 991.

368 *See* Katharine Gibbs Sch. Inc. v. FTC, 612 F.2d 658, 658 (2d Cir. 1979).

369 *See Am. Fin. Servs.*, 767 F.2d at 990–91; *supra* notes 359–62.

preemption exemption for state laws that provide equal or greater protection for consumers. In this way, the FTC can fortify its data security TRR, and better guarantee that judicial review will not end in rebuke.

CONCLUSION

In an era where consumer information is treated as a prized commodity, data breaches pose a serious threat to consumers and companies alike. Using its broad Section 5(a) authority, the FTC has undertaken an effort to protect consumers by policing unfair and deceptive data security practices. For nearly two decades, the Commission has largely proceeded under a quasi-judicial approach. Following a company's culpable data breach, the Commission conducts an investigation, files an administrative complaint and extends a settlement offer. This enforcement model, appropriate at the dawn of the digital age, is in need of revision. Using the power Congress granted to it, the FTC should focus its efforts on promulgating a data security trade regulation rule. The benefits of doing so outweigh the costs. A data security rule stands to enhance the Commission's capacity to protect consumers, conserve agency resources, and provide more definite guidance to the regulated community.

Despite the FTC's reluctance to invoke its Magnuson-Moss rulemaking authority, it is capable of crafting an effective data security rule that can withstand judicial review. The Commission has confronted issues of data security for nearly two decades. It has brought enforcement actions, engaged the public, conducted research, and in the process, accumulated a level of expertise that is unrivaled on the federal regulatory plane. Critical to any unfairness action, the FTC has articulated a uniquely flexible conception of consumer data breach injuries that, when incorporated into a hard and fast rule, will go lengths in protecting consumer interests. Although hackers will always find ways to exploit digital vulnerabilities, the FTC has demonstrated that it is a regulatory force to be reckoned with. As such, the FTC should look to its present powers, resurrect its Magnuson-Moss rulemaking authority, and promulgate a trade regulation rule that specifies the parameters of unlawful data security.

IAN M. DAVIS*

* Much gratitude is due for the (successful) completion of this work. In chief, a thank you to Thomas Arthur for sparking my interest in administrative law and elevating the quality of my work product. To Martin Semel and Allan Davis for initiating me into the legal profession. To Dr. Cas Mudde for showing to me the practical value of academic scholarship. To Bob Cash for shaping the mold. And finally, to John Parker Jr. and

George Brewster for their diligent editing expertise.