COLUMBIA LAW REVIEW FORUM

VOL. 120 JUNE 1, 2020 PAGES 134–152

# WHEN CONGRESS MAKES NO POLICY CHOICE: THE CASE OF FTC DATA SECURITY ENFORCEMENT

*Tyler Becker* *

*For twenty-five years, the Federal Trade Commission (FTC) has brought enforcement actions against companies for data breaches using its statutory authority under Section 5 of the FTC Act to police "unfair or deceptive acts or practices." While the Commission originally brought cases under the "deceptive" prong of Section 5, more recent cases have been brought under the vague "unfairness" prong. These cases allege that a company that has experienced a data breach engaged in "unfair" acts or practices by failing to adopt "reasonable" data security measures. All but one of the cases were settled outside of court through consent decrees or the FTC dropping the case. In 2018, the Eleventh Circuit found the FTC overstepped its authority in the one case that did not settle,* LabMD, Inc. v. FTC. *The decision called into question the FTC's data security enforcement practices and, specifically, its use of a vague "reasonableness" standard in its consent decrees. Now, the FTC has rethought its approach to data security enforcement and asked Congress to clarify the FTC's authority.*

*This Comment argues that the FTC has failed to provide fair notice to regulated parties about what data security practices businesses must engage in to avoid enforcement actions. Further, the Comment argues that Congress must make a policy choice in the data security space and specify a private standard that the FTC must use to evaluate data security practices. If not, regulated parties should begin commenting on complaints, orders, and consent decrees to induce the Commission to further clarify what "reasonable," and therefore "fair," data security practices entail.*

* Juris Doctor 2020, Columbia Law School. The author would like to thank Professor Philip Hamburger for discussing ideas and providing guidance with respect to this Comment. The author would also like to thank the staff of the *Columbia Law Review* for expert editorial support.

## INTRODUCTION

Since 1995, the Federal Trade Commission (FTC) has used its jurisdiction to police "unfair or deceptive acts or practices"[1] to force companies to adopt data security measures capable of protecting consumer data.[2] However, the FTC's authority in the data security enforcement context came under scrutiny in *LabMD, Inc. v. FTC*, a 2018 Eleventh Circuit decision that invalidated the FTC's attempted enforcement action against LabMD, a medical laboratory that suffered a data breach exposing patient records.[3] Finding that the FTC's proposed consent order "commanded LabMD to overhaul and replace its data-security program to meet an indeterminable standard of reasonableness," the court held that the FTC could not enforce its order.[4] Specifically, the court cited the lack of specificity of what data security measures LabMD failed to take prior to the breach and would be ordered to take if the company agreed to the consent order as the reasons for its decision.[5]

For the FTC, *LabMD* represented a significant defeat. Prior to the decision, the FTC used its authority under the "unfairness" prong of Federal Trade Commission Act Section 5 to bring cases against companies for failing to adopt what the Commission considers "reasonable" data security measures without any additional specificity.[6] Therefore, the *LabMD* decision called into question the FTC's entire data security enforcement practice. In December 2018, the agency held a rare public hearing on the topic.[7] In 2019, FTC Chairman Joseph Simons asked Congress for "targeted rule-making authority" in the data security context governed by "clear and specific rules."[8] And, the FTC claims to be making its data security orders

---

1. 15 U.S.C. § 45(a)(1) (2018) ("Unfair methods of competition in or affecting commerce, and unfair or deceptive acts or practices in or affecting commerce, are hereby declared unlawful.").

2. See Daniel J. Solove & Woodrow Hartzog, The FTC and the New Common Law of Privacy, 114 Colum. L. Rev. 583, 598–99 (2014) [hereinafter Solove & Hartzog, Common Law of Privacy].

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

4. Id. at 1236.

5. Id.

6. See FTC, Commission Statement Marking the FTC's 50th Data Security Settlement 1 (2014) [hereinafter 50th Settlement Statement], https://www.ftc.gov/system/files/documents/cases/140131gmrstatement.pdf [https://perma.cc/U289-SSEH].

7. See Press Release, FTC, FTC Announces Sessions on Consumer Privacy and Data Security as Part of Its Hearings on Competition and Consumer Protection in the 21st Century (Oct. 26, 2018) [hereinafter FTC Announces], https://www.ftc.gov/news-events/press-releases/2018/10/ftc-announces-sessions-consumer-privacy-data-security-part-its [https://perma.cc/R6GP-73CW].

8. See Diane Bartz, Privacy-Minded U.S. Lawmakers Divided over Giving More Powers to FTC, Reuters (May 8, 2019), https://www.reuters.com/article/us-usa-congress-privacy/privacy-minded-u-s-lawmakers-divided-over-giving-more-powers-to-ftc-idUSKCN1SE2HS [https://perma.cc/LU36-2REB].

more specific[9]—including almost entirely eliminating the word "reasonableness" from its consent decrees.[10] However, the Commission has still provided little guidance on what data security practices constitute an "unfair" practice within the ambit of the FTC's statutory enforcement authority to remedy, and still continues to use the vague "reasonableness" standard in its complaints when bringing enforcement actions.[11]

Congress could fix this problem by specifying the FTC's data security enforcement authority, but so far it has failed to do so. And there is little hope for reform in the near future. Following California's passage of a data privacy law in 2018 (the California Consumer Privacy Act (CCPA)) and the implementation of the General Data Protection Regulation (GDPR) in the European Union, the current focus in Congress is on data *privacy*—"user[] . . . control over how businesses collect, use, and share their information"—and not data *security*—"prevent[ing] unauthorized parties from accessing, altering, or rendering unavailable [consumers'] data."[12] As a result, regulated parties—really any business operating online or using electronic records—are likely to continue to face the risk of FTC data security enforcement actions without clarified standards. Congress has failed "to make the 'important policy choices'"[13] with respect to data

---

9. See Andrew Smith, New and Improved FTC Data Security Orders: Better Guidance for Companies, Better Protection for Consumers, FTC (Jan. 6, 2020), https://www.ftc.gov/news-events/blogs/business-blog/2020/01/new-improved-ftc-data-security-orders-better-guidance [https://perma.cc/74RK-KHCT].

10. Randy Milch & Sam Bieler, A New Decade and New Cybersecurity Orders at the FTC, Lawfare (Jan. 29, 2020), https://www.lawfareblog.com/new-decade-and-new-cybersecurity-orders-ftc# [https://perma.cc/Q463-CKGU].

11. See infra note 50 and accompanying text.

12. See Jeff Kosseff, Congress Is Finally Tackling Privacy! Now Let's Do Cybersecurity., Slate (Dec. 3, 2019), https://slate.com/technology/2019/12/congress-national-privacy-law-cybersecurity.html [https://perma.cc/8S8P-4CVU] ("[C]ybersecurity has taken a backseat to privacy in our current national debate, in part because policymakers often conflate the issues and claim to be addressing both.").

13. Gundy v. United States, 139 S. Ct. 2116, 2145 (2019) (Gorsuch, J., dissenting) (quoting Indus. Union Dep't, AFL–CIO v. Am. Petroleum Inst., 448 U.S. 607, 676 (1980) (Rehnquist, J., concurring)). The fact that the FTC derives much of its statutory authority to regulate data security from Section 5's "unfairness" prong is particularly concerning given that multiple Supreme Court Justices now support a revival of the nondelegation doctrine. See Damon Root, Kavanaugh Joins Gorsuch in Fight to Revive Nondelegation Doctrine, Reason (Nov. 25, 2019), https://reason.com/2019/11/25/kavanaugh-joins-gorsuch-in-fight-to-revive-nondelegation-doctrine/?amp [https://perma.cc/EL7M-923R]. While this Comment takes no position on whether the FTC's data security enforcement is a nondelegation issue, data security is an area in which there is little dispute that regulation is needed, Congress has failed to adequately define authority to regulate, and an administrative agency has taken over the regulation using vague statutory authority and standards. Data security is a field in which Congress has provided no policy choice, and as a result regulated parties are forced to contend with an administrative enforcement system that fails to provide adequate notice of the regulatory requirements to businesses. See infra Part II.

security regulation and has left regulated parties to contend with ad hoc FTC enforcement guided by both vague statutory authority ("unfairness") and vague standards ("reasonableness").

This Comment argues that regulated parties lack adequate notice of what the FTC considers "unfair" data security practices given the realities of the FTC's current enforcement mechanisms, and that Congress should provide clearer data security standards as part of a larger privacy bill. Absent congressional action, regulated parties should begin commenting on the FTC's complaints, orders, and consent decrees to force the Commission's data security staff to clarify what data security practices companies must adopt to avoid FTC enforcement actions. Part I discusses the FTC's current data security enforcement practices, the *LabMD* decision that called them into question, and the Commission's reaction to *LabMD*. Part II identifies the problem with the current approach and argues that the changes the FTC has made post-*LabMD* fail to sufficiently clarify what the FTC considers "reasonable" data security practices. Part III provides two potential solutions, one involving congressional action and one involving congressional inaction, to provide regulated parties notice of what "reasonable" data security means.

## I. FTC DATA SECURITY ENFORCEMENT PRACTICE BEFORE AND AFTER *LABMD*

The FTC has brought seventy cases alleging inadequate data security practices since 1995.[14] Section I.A provides a description of the statutory authority that the FTC uses for data security enforcement. Then, section I.B describes *LabMD* and explains why the case called into question the FTC's data security enforcement practice. Section I.C discusses the FTC's reaction to *LabMD*.

### A. *The FTC's Claimed Statutory Authority to Regulate Data Security*

The FTC uses its statutory authority to police "unfair or deceptive acts or practices"[15] in order to make companies adopt data security measures with the goal of protecting consumer data.[16] When the FTC is alerted to a data breach and has "'reason to believe' the law is being violated,"[17] the FTC has two methods for bringing an enforcement action against the company responsible for the data's safekeeping, and two statutory provisions under which it can bring the action.

---

14. Data Security, FTC, https://www.ftc.gov/tips-advice/business-center/privacy-and-security/data-security [https://perma.cc/7ZZ3-AKLJ] (last visited Apr. 23, 2020).

15. 15 U.S.C. § 45(a)(1) (2018).

16. Solove & Hartzog, Common Law of Privacy, supra note 2, at 598–99.

17. A Brief Overview of the Federal Trade Commission's Investigative, Law Enforcement, and Rulemaking Authority, FTC (Oct. 2019), http://www.ftc.gov/about-ftc/what-we-do/enforcement-authority [https://perma.cc/QC49-QABV].

First, the FTC can choose whether to bring an enforcement action in an administrative proceeding or in federal court.[18] In the data security context, the FTC rarely brings cases in court and instead uses administrative adjudication to force defendants into consent decrees.[19]

Second, and more relevant to the data security context, is what prong the FTC brings the action under. When the Commission decides to initiate an enforcement action, the FTC chooses whether to bring the enforcement action under the "deceptive" or "unfairness" prongs of Section 5 of the FTC Act.[20] If the Commission brings the enforcement action under the "deceptive" prong, the FTC looks at the statements a business that experiences a data breach has made to consumers about privacy protection, and alleges the business violated the privacy standards it promised to consumers (and, therefore, "deceived" them).[21] For the "deceptive" prong to be violated, the FTC has said in its Policy Statement on Deception that the alleged deception must be "material" to consumers, meaning "consumers are likely to have chosen differently but for the deception."[22] If the FTC brings an enforcement action under the "unfairness" prong, the Commission alleges that the business engaged in an unfair trade practice that allowed it to gain an advantage over competitors by not offering "reasonable" data security to consumers.[23]

While the early data security enforcement actions were brought under the "deceptive" prong, recent controversial cases like *LabMD* have been brought under the "unfairness" prong, which suggests a desire on the part of the FTC to expand its enforcement power in the data security area.[24] This tracks with the change from the early period of the FTC's data security enforcement when the FTC "encouraged self-regulation" during which "the companies themselves . . . create[d] their own rules, and the FTC . . . enforce[d] them" using the "deceptive" prong of Section 5.[25] In recent

18. Solove & Hartzog, Common Law of Privacy, supra note 2, at 609.

19. See Gerard Stegmaier & Wendell Bartnick, Psychics, Russian Roulette, and Data Security: The FTC's Hidden Data-Security Requirements, 20 Geo. Mason L. Rev. 673, 690 (2013).

20. See id. at 674–75.

21. Id. at 674.

22. See FTC, Policy Statement on Deception 1 (1983), https://www.ftc.gov/system/files/documents/public_statements/410531/831014deceptionstmt.pdf [https://perma.cc/WP9J-S728].

23. See Geoffrey A. Manne & Kristian Stout, When "Reasonable" Isn't: The FTC's Standardless Data Security Standard, 15 J.L. Econ. & Pol'y 67, 74–75 (2019); see also FTC Policy Statement on Unfairness, FTC (Dec. 17, 1980), https://www.ftc.gov/public-statements/1980/12/ftc-policy-statement-unfairness [https://perma.cc/VW4P-HL6B]. In 2019 and after the *LabMD* decision, the FTC began eliminating the word "reasonableness" from its consent decrees. Milch & Bieler, supra note 10.

24. See LabMD, Inc. v. FTC, 894 F.3d 1221, 1226 (11th Cir. 2018); Stegmaier & Bartnick, supra note 19, at 674–75 & nn.11–12.

25. Solove & Hartzog, Common Law of Privacy, supra note 2, at 599.

years, the FTC has been using the "unfairness" prong of Section 5 to bring cases against companies for failing to adopt what the Commission considers "reasonable" data security measures.[26] This "reasonableness" standard requires a company to adopt "data security measures . . . [that are] reasonable and appropriate in light of the sensitivity and volume of consumer information it holds, the size and complexity of its business, and the cost of available tools to improve security and reduce vulnerabilities."[27] But, what are "reasonable" data security measures? As is discussed next, the *LabMD* case shows that the FTC did not make this clear.

### B. *The* LabMD *Decision*

LabMD, Inc. was a "medical laboratory that previously conducted diagnostic testing for cancer . . . [that] used medical specimen samples, along with relevant patient information, to provide physicians with diagnoses."[28] The company was a growing small business with thirty employees and four million dollars in annual sales prior to the litigation.[29] Then, LabMD's billing manager used LimeWire on her computer to download music.[30] LimeWire is a "peer-to-peer file-sharing application" that makes anything within a "folder selected for downloads . . . available to others on the network."[31] An employee from a data security firm was able to log onto LabMD's network because of the billing manager's mistake and download a file containing the personal information of 9,300 LabMD patients, which included their "names, dates of birth, social security numbers, laboratory test codes, and, for some, health insurance company names, addresses, and policy numbers."[32]

After LabMD refused to purchase the data security firm's services to help investigate the data breach, the firm reported the breach to the FTC.[33] The FTC issued a complaint against LabMD alleging that the company engaged in "'an unfair act or practice' . . . by 'engag[ing] in a number of practices that, taken together, failed to provide *reasonable* and *appropriate* security for personal information on its computer networks.'"[34]

---

26. See 50th Settlement Statement, supra note 6.

27. Id.

28. *LabMD*, 894 F.3d at 1224.

29. See Dune Lawrence, A Leak Wounded This Company. Fighting the Feds Finished It Off, Bloomberg Businessweek (Apr. 25, 2016), https://www.bloomberg.com/features/2016-labmd-ftc-tiversa [https://perma.cc/X7UN-TZ3Z].

30. See *LabMD*, 894 F.3d at 1224; Lawrence, supra note 29.

31. *LabMD* and the Future of FTC Data Privacy Regulation, Dentons (July 17, 2018), https://www.dentons.com/en/insights/articles/2018/july/17/labmd-and-the-future-of-ftc-data-privacy-regulation [https://perma.cc/7RLZ-DNHD].

32. *LabMD*, 849 F.3d at 1224.

33. Id. at 1224–25. For an account of the controversial practices of Tiversa, the data security firm responsible for breaching LabMD's network, including faking data breaches to promote its services, see generally Lawrence, supra note 29.

34. *LabMD*, 894 F.3d at 1225 (alteration in original) (emphasis added).

LabMD was given an ultimatum: Go through costly litigation, or settle and sign a consent decree to revamp the company's data security system and subject the company to FTC oversight.[35] LabMD's founder chose the former option because the company feared doctors who used the company would think "that LabMD had been lax in protecting patient data and kill his business."[36]

A protracted litigation ensued, and ultimately the Eleventh Circuit found the FTC overstepped its authority in the case.[37] Concerned that the FTC's "cease and desist order . . ." does not instruct LabMD "to stop committing a specific act or practice" and instead "commands LabMD to overhaul and replace its data-security program to meet an indeterminable standard of reasonableness," the Eleventh Circuit found the FTC's order "unenforceable."[38]

The decision was perceived as having a significant impact on the FTC's data security enforcement practice. Prior to *LabMD*, the FTC had "brought more than 60 cases related to data security. In all but one, the companies involved . . . settled, signing consent decrees that in many cases require 20 years of security audits by an outside firm and sometimes fines."[39] Many of these cases were brought under the vague "reasonableness" standard the Eleventh Circuit found so problematic in *LabMD*. The next section discusses the FTC's reaction to the decision.

### C. *FTC Data Security Enforcement Post-*LabMD

*LabMD* brought attention to many of the problems with the FTC's data security enforcement practices, and the Commission recognized this fact. After *LabMD*, the Commission scheduled a public hearing "to examine the FTC's authority to deter unfair and deceptive conduct in data security . . . matters."[40] Following the hearing, the FTC engaged in a public campaign to lobby Congress to provide the agency more authority over data security (and privacy) issues. The FTC has argued that the United States lags behind other western countries in its approach to data security. In an April 2019 congressional hearing, FTC Chairman Joseph Simons said that while the FTC only has forty employees dedicated to data security enforcement, the United Kingdom has 500.[41] As a result, the Commission

35. See Lawrence, supra note 29.

36. Id.

37. See *LabMD*, 894 F.3d at 1237.

38. Id. at 1236.

39. See Lawrence, supra note 29.

40. FTC Announces, supra note 7.

41. See Harper Neidig, FTC Says It Only Has 40 Employees Overseeing Privacy and Data Security, The Hill (April 3, 2019), https://thehill.com/policy/technology/437133-ftc-says-it-only-has-40-employees-overseeing-privacy-and-data-security [https://perma.cc/5TBV-QGV6].

has asked Congress to provide additional funding for data security (and privacy) enforcement staff, which the Commission hopes will provide funding for at least 160 new staffers who can help the Commission bring more cases.[42] The Commission has also asked for "comprehensive data security legislation . . . that would be enforced by the FTC."[43] Specifically, Simons has asked for what he terms "targeted rule-making authority" in the data security context governed by "clear and specific rules."[44] He has implored Congress to avoid "dump[ing] [the] question" of what rules to create on the FTC by granting the agency "broad rule-making authority."[45] In other words, Simons is likely looking to avoid a repeat of *LabMD* by getting clear authority from Congress to regulate data security.

Additionally, the FTC claims to be making its data security orders more "specific."[46] In a blog post, the Commission notes that the orders "continue to require that the company implement a comprehensive, process-based data security program, and [now] they require the company to implement specific safeguards to address the problems alleged in the complaint" such as "yearly employee training, access controls, monitoring systems for data security incidents, patch management systems, and encryption."[47] This has included avoiding using the word "reasonable" in the "operative information security language" of the Commission's data security consent decrees issued in 2019.[48] Of course, this is unsurprising given the *LabMD* court's concern that the Commission tried to make the company implement a data security program "'reasonably designed' to the Commission's satisfaction."[49] However, the FTC continues to use "reasonableness" in its complaints alleging unfair data security practices.[50] This begs the question to which this Comment turns to next: Do regulated parties have notice about what the FTC considers "unreasonable," and

42. See id.

43. FTC Testifies Before Senate Commerce Subcommittee About the Agency's Work to Protect Consumers, Promote Competition, and Maximize Resources, FTC (Nov. 27, 2018), https://www.ftc.gov/news-events/press-releases/2018/11/ftc-testifies-senate-commerce-subcommittee-about-agencys-work [https://perma.cc/P2EA-CJ8D].

44. See Bartz, supra note 8.

45. Id.

46. Smith, supra note 9.

47. Id.

48. Milch & Bieler, supra note 10.

49. LabMD, Inc. v. FTC, 894 F.3d 1221, 1230 (11th Cir. 2018).

50. See, e.g., Complaint for Permanent Injunction and Other Relief at 11, FTC v. Equifax, Inc., No. 19-cv-03297-TWT (N.D. Ga. July 22, 2019), https://www.ftc.gov/system/files/documents/cases/172_3203_equifax_complaint_7-22-19.pdf [https://perma.cc/HC9F-XGTL] ("Defendant engaged in a number of practices that, taken together, failed to provide reasonable security for the massive quantities of sensitive personal information stored within Defendant's computer network."); Complaint for Civil Penalties, Permanent Injunction, and Other Equitable Relief at 9, United States v. Unixiz, Inc., No. 19-cv-02222 (N.D. Cal. Apr. 24, 2019) ("Defendants engaged in a number of practices that, taken together, failed to provide reasonable and appropriate data security to protect the personal information collected from consumers . . . .").

therefore "unfair," data security practices that are within the Commission's statutory authority to regulate?

## II. REGULATED PARTIES LACK NOTICE OF WHAT CONSTITUTES "UNFAIR" DATA SECURITY PRACTICES

Assuming the FTC has statutory authority to regulate data security under the "unfairness" prong and can make data security policy by adjudication, the Commission still must provide "fair notice" of what constitutes "reasonable," and therefore "fair," data security practices.[51] Even when looked at in the most positive light, the FTC has not provided fair notice to regulated parties about what data security measures the Commission considers appropriate. This is a result of (1) the lack of bright-line rules for when a party can be said to have engaged in "unreasonable," and therefore "unfair," data security practices and (2) the lack of information in the adjudicatory documents on the FTC's website. Each of these will be discussed in turn.

### A. *Balancing Test Invites Arbitrary Enforcement*

The FTC does not use bright-line rules in the data security context. In other words, there are no per se unreasonable data security practices. The Commission emphasizes that "it does not require perfect security" and "the mere fact that a breach occurred does not mean that a company has violated the law."[52] Instead, the Commission will use a balancing test to determine whether to bring an action when a breach does occur. Before filing a complaint, the FTC will balance the costs and benefits of security measures that would have prevented the breach to determine whether the company behaved unreasonably by failing to adopt those measures, making the company's behavior "unfair" within the meaning of the FTC Act.[53]

While such a balancing test is common in administrative proceedings and allows agencies to use their prosecutorial discretion, the way the FTC pursues companies alleged to have engaged in unreasonable data security practices differs from many other administrative adjudications given its overly post hoc nature.[54] When a data breach occurs, the FTC decides whether or not to file a complaint based "only [on] those remedial measures it claim[s] would address the specific breach at issue," and whether the

---

51. See Stegmaier & Bartnick, supra note 19, at 689.

52. See 50th Settlement Statement, supra note 6, at 1.

53. See Manne & Stout, supra note 23, at 83.

54. See Alan Charles Raul & Vivek K. Mohan, United States, *in* The Privacy, Data Protection & Cybersecurity L. Rev. 376 (Alan Charles Raul ed., 5th ed. 2018), https://www.sidley.com/-/media/publications/united-states-fifth-edition.pdf?la=en [https://perma.cc/8LLV-AFWU] ("The US privacy system has a relatively flexible and non-prescriptive approach, relying more on post hoc government enforcement . . . and on the corresponding deterrent value of such enforcement . . . than on detailed prohibitions and rules.").

company's failure to institute those measures prior to the breach was unreasonable.[55] The FTC has the benefit of hindsight: The data breach happened. But what the company is prosecuted for is not the data breach itself; it is the specific measures the company failed to take that would have prevented the breach.

When determining whether to bring a data security case, the agency "ignores the overall compliance burden on a company to avoid excessive risk without knowing, ex ante, which specific harm(s) might occur."[56] The FTC does not consider the overall risks the company faced and whether the failure to address the specific risk, when considered with all the others, was unreasonable.[57] Instead, the Commission's data security staff make a post hoc determination of reasonableness without a "clear . . . baseline and a rigorous evaluation of the contribution of the company's practices to any deviation from it."[58] As a result, companies are penalized for the size of the data breach, not for their engagement in "unfair" or "unreasonable" data security practices.

For example, in *LabMD*, the Commission admitted that the company had a comprehensive data security program that "included 'training, firewalls, network monitoring, password controls, access controls, anti-virus, and security-related inspections.'"[59] But because the program did not protect against the *specific* LimeWire risk that caused the breach, the FTC brought an enforcement action against the company.[60] There was no consideration of the percentage chance such a risk would have been ex ante (which was actually very low), nor credit given to LabMD for having a comprehensive data security program.[61] Instead, the Commission waited until the breach occurred and then determined LabMD behaved unreasonably with this benefit of hindsight.[62]

Such a post hoc approach invites arbitrary enforcement given that the reasonableness of ex ante data security measures is not the reason the FTC actually brings a case; it is the data breach itself that causes the FTC to become involved. As some scholars have described, the FTC "infer[s] a high prior probability, or even a certainty, of insufficient security from a

55. See Manne & Stout, supra note 23, at 79.

56. Id.

57. Id. at 79–80.

58. Id. at 80.

59. LabMD, Inc. v. FTC, 894 F.3d 1221, 1224 n.4 (11th Cir. 2018).

60. See id. at 1230 ("Because LabMD failed to employ . . . [certain security] measures, the Commission's theory goes, LimeWire was able to be installed on the billing manager's computer. LabMD's policy forbidding employees from installing programs like LimeWire was insufficient.").

61. See Manne & Stout, supra note 23, at 79–80 ("[T]he FTC conducted an inappropriately post hoc assessment that considered only those remedial measures it claimed would address the specific breach at issue. But this approach ignores the overall compliance burden on a company to avoid excessive risk without knowing, ex ante, which specific harm(s) might occur.").

62. Cf. *LabMD*, 894 F.3d at 1230 n.27.

single, post hoc occurrence . . . [and] imposes an effective *strict liability* regime on companies that experience a breach . . . ."[63] Companies that fail to adopt anything resembling "fair" or "reasonable" data security practices may never face FTC enforcement actions if they are lucky enough to never experience a data breach. Companies that have comprehensive data security programs, such as LabMD, may face FTC enforcement actions because a breach occurs. The single biggest factor in the "balancing test" employed by the FTC when deciding to bring a case is the breach that occurred, even if the company could not have, or reasonably would not have, considered the risk prior to the breach. Such an approach would be more acceptable if the FTC provided notice about what the ex ante "reasonable" data security measures are. But the Commission has failed on that metric, as is discussed next.

### B. *FTC Data Security Complaints, Consent Orders, and Security Assessments Provide Little Information*

Even if parties were to look at the FTC's published records in data security cases, the parties would find very little information about what the Commission considers appropriate data security practices. This is the result of the practical realities companies face following a data breach that cause quick settlements with the FTC, the lack of specificity in the materials the FTC makes available about its enforcement practices, and the fact that FTC complaints only detail what data security practices the FTC considers "unfair" post hoc (as in, after a data breach).

1. *Practical Realities Make Settlements the Norm, Leading to Few Well-Reasoned Documents Explaining "Fair" or "Reasonable" Data Security Practices.* — First, the practical realities for companies plagued with a data breach contribute to the limited nature of available documents on what the FTC considers appropriate data security practices. Companies exposed to data breaches typically want to mitigate the impact to their business and quickly settle with the FTC.[64] In fact, complaints and consent orders are often released on the same day, as companies already facing a data breach choose to settle before there is any public mention of an FTC complaint that could further harm their business.[65] As a result, there is a lack of well-reasoned

63. Manne & Stout, supra note 23, at 80 (emphasis added).

64. See Gina Stevens, Cong. Research Serv., R43723, The Federal Trade Commission's Regulation of Data Security Under Its Unfair or Deceptive Acts or Practices (UDAP) Authority 7 (2014) (noting that "most of the FTC's privacy and data security cases . . . [are] resolved with settlements or abandoned"); *LabMD* and the Future of FTC Data Privacy Regulation, supra note 31 (explaining that "[t]ypically, when an organization receives a Complaint from the FTC they choose to negotiate toward a settlement" because the alternative "legal battles are costly and time-consuming" and "[l]osing at any level will result in the issuance of a coercive order").

65. See, e.g., ASUSTeK Computer Inc.: Case Timeline, FTC (July 28, 2016), https://www.ftc.gov/enforcement/cases-proceedings/142-3156/asustek-computer-inc-matter [https://

adjudicatory decisions by the Commission. The parties must rely on complaints, investigatory notices, and consent orders on the FTC's website to get an idea of what the Commission considers to be "fair" or "reasonable" data security practices.[66] This limited number of available documents contributes to a lack of fair notice to parties about what data security practices the FTC expects companies to adopt.

2. *Available Documents Lack Specificity.* — Second, the documents that do exist lack specificity about what the Commission considers appropriate data security practices. FTC complaints and investigatory notices only contain boilerplate language and make conclusory statements accusing companies of having "unreasonable" data security practices that led to data breaches.[67] The complaints include a list of what the companies did *not* do to protect consumer data with conclusory statements that the practices are data security measures the companies should reasonably have taken.[68] For example, in its complaint against HTC America, the FTC accused the company of: "(a) fail[ing] to implement an adequate program to assess the security of products it shipped to consumers; (b) fail[ing] to implement adequate privacy and security guidance or training for its engineering staff; . . .

---

perma.cc/9HGP-TJCX] (listing the dates of both the "Complaint" and the "Agreement Containing Consent Order" as February 23, 2016); TRENDnet, Inc.: Case Timeline, FTC (Feb. 7, 2014) [hereinafter TRENDnet Timeline], https://www.ftc.gov/enforcement/cases-proceedings/122-3090/trendnet-inc-matter [https://perma.cc/GR3X-PWP9] (listing the dates of both the "Complaint" and the "Agreement Containing Consent Order" as September 4, 2013); see also Lawrence, supra note 29 (describing how all but one company settled with the FTC for data security violations rather than risk protracted litigation).

66. See Stevens, supra note 64, at 6–7 (noting that because of the prevalence of consent orders in data security enforcement actions, "there are few judicial decisions addressing the FTC's authority to regulate the data security practices of companies which have suffered a data breach"); Manne & Stout, supra note 23, at 75.

67. See, e.g., *LabMD*, 894 F.3d at 1230 n.27 (describing the allegations in the FTC's complaint as "unspecific and perhaps boilerplate").

68. See, e.g., Complaint at 7–8, ASUSTeK Computer, Inc., FTC File No. 142 3156, No. C-4587 (F.T.C. July 28, 2016) [hereinafter ASUSTeK Complaint], https://www.ftc.gov/system/files/documents/cases/1607asustekcmpt.pdf [https://perma.cc/4ANA-R92C] (listing supposedly unreasonable data security practices including failing to "perform reasonable and appropriate code review" and "implement readily-available, low-cost protections against well-known and reasonably foreseeable vulnerabilities"); Complaint at 4–5, TRENDnet, Inc., FTC File No. 122 3090, No. C-4426 (F.T.C. Feb. 7, 2014), https://www.ftc.gov/system/files/documents/cases/140207trendnetcmpt.pdf [https://perma.cc/2ZM3-U7SA] (listing supposedly unreasonable data security practices including that "respondent . . . failed to employ reasonable and appropriate security in the design and testing of the software that it provided consumers for its IP cameras" and "implement reasonable guidance or training for any employees" involved in testing their security); Complaint at 3, LabMD, Inc., FTC File No. 102 3099, No. 9357 (F.T.C. Aug. 29, 2013) [hereinafter LabMD Complaint], http://www.ftc.gov/sites/default/files/documents/cases/2013/08/130829labmdpart3.pdf [https://perma.cc/4C2T-DPLD] (listing supposedly unreasonable data security practices including "not us[ing] readily available measures to identify commonly known or reasonably foreseeable security risks and vulnerabilities on its networks" and asserting, without mention of the cost, that LabMD "could have corrected its security failures at relatively low cost").

[and] (d) fail[ing] to follow well-known and commonly-accepted secure programming practices . . . ."[69] These accusations are written in general language and lack the specificity a party trying to comply with FTC data security regulations could look to in order to find what the standards are. How does the FTC define "adequate privacy and security guidance," for example? What about "well-known and commonly-accepted secure programming practices"? As a result of this general language, the complaints provide little guidance on what constitutes appropriate data security measures companies can take to avoid FTC enforcement actions against them.

The complaints also provide little guidance to regulated parties because they include no mention of the weight of the individual "reasonable" practices the company did not take. Invariably, the complaints include a sentence along these lines: "Respondent has engaged in a number of practices that, taken together, failed to provide reasonable security . . . ."[70] This remains the case after *LabMD*.[71] Even if a party could discern a clear practice required by an FTC complaint, the agency does not assert that failure to follow that practice will be deemed unlawful in the next case.[72] It all depends on the practices "taken together," which is a case-by-case determination.[73]

Consent decrees are another place regulated parties may hope to get information about what the Commission considers to be appropriate data security practices, but they are similarly deficient. When a party settles with the FTC, the FTC typically imposes a twenty-year consent order that requires continuous monitoring by the FTC and annual or biennial privacy assessments.[74] Because most parties choose to settle with the FTC, every data security case (with the exception of *LabMD*) has one on the FTC's website.[75] However, "[e]ach clause and provision [of these consent decrees]

---

69. Complaint at 2, HTC America, Inc., FTC File No. 122 3049, No. C-4406 (F.T.C. July 2, 2013), https://www.ftc.gov/sites/default/files/documents/cases/2013/07/130702htccmpt.pdf [https://perma.cc/6UPY-Q2G3].

70. See, e.g., ASUSTeK Complaint, supra note 68, at 7; see also LabMD Complaint, supra note 68, at 3 (substituting "reasonable security" for "reasonable and appropriate security").

71. See, e.g., Grago, FTC Doc. No. 172 3003, No. C-4678, at 3–4 (F.T.C. July 2, 2019), https://www.ftc.gov/system/files/documents/cases/172_3003_c4678_clixsense_complaint_7-2-19.pdf [https://perma.cc/9XB2-FZWR] ("Since 2010, Respondent has engaged in a number of *unreasonable* security practices that led to the breach . . . [and] caused or are likely to cause substantial consumer injury." (emphasis added)).

72. See Stegmaier & Bartnick, supra note 19, at 693.

73. Id.

74. See Woodrow Hartzog & Daniel J. Solove, The Scope and Potential of FTC Data Protection, 83 Geo. Wash. L. Rev. 2230, 2297 (2015) [hereinafter Hartzog & Solove, Scope and Potential].

75. See Lawrence, supra note 29.

is carefully worded to limit its scope and cabin any corporate liability."[76] The orders are negotiated by lawyers for the corporation and the FTC, and are written in a manner that includes no admission of guilt.[77] And, like the complaints, the orders contain general language about what the Commission considers to be appropriate data security measures that will bring the corporation into compliance.[78]

Another area where parties could look for guidance are the third-party privacy assessments that companies subject to consent orders are required to undergo annually or biannually.[79] However, there are two problems with these documents. First, they can only be obtained through a Freedom of Information Act request; they are not available on the agency's website for regulated parties to view.[80] Second, because these assessments can be released to the public, they contain little information about what the company is doing, or what the FTC is making the company do, to

---

76. Joseph Jerome, Can FTC Consent Orders Effectively Police Privacy?, Int'l Ass'n of Privacy Profs. (Nov. 27, 2018), https://iapp.org/news/a/can-ftc-consent-orders-police-privacy [https://perma.cc/N8A6-3338].

77. See id. For the argument that it is improper to say that FTC consent orders provide "fair notice" because of their status as contracts, but parties still have "fair notice" of the FTC's data security practices from the complaints the FTC files, see generally Vladimir J. Semendyai, Note, Due Process and the FTC's Fair and Reasonable Approach to Data Protection, 84 Geo. Wash. L. Rev. Arguendo 51 (2016).

78. See, e.g., ASUSTeK, Inc., FTC File No. 142 3156, No. C-4587, at 5 (F.T.C. July 18, 2016) (decision and order), https://www.ftc.gov/system/files/documents/cases/1607asustekdo.pdf [https://perma.cc/FP96-HXYP] (mandating "[t]he design and implementation of *reasonable* safeguards to control the risks identified through risk assessment, including through *reasonable and appropriate* software security testing techniques" (emphasis added)); TRENDnet, Inc., FTC File No. 122 3090, No. C-4426, at 5 (F.T.C. Jan. 16, 2014) (decision and order), https://www.ftc.gov/system/files/documents/cases/140207trendnetdo.pdf [https://perma.cc/EJF8-6L5R] (requiring "*reasonable* safeguards to control the risks identified through the risk assessments, including . . . *reasonable and appropriate* software security testing techniques" and "*reasonable* steps to select and retain service providers capable of maintaining security practices" (emphasis added)); Rite Aid Corp., FTC File No. 072 3121, No. C-4308, at 3–4 (F.T.C. Nov. 22, 2010) (decision and order), https://www.ftc.gov/sites/default/files/documents/cases/2010/11/101122riteaiddo.pdf [https://perma.cc/N5AF-XQJK] (requiring "the development and use of *reasonable* steps to select and retain service providers capable of appropriately safeguarding personal information they receive from Respondent, and requiring service providers by contract to implement and maintain *appropriate* safeguards" (emphasis added)).

79. See Kashmir Hill, So, What Are These Privacy Audits that Google and Facebook Have to Do for the Next 20 Years?, Forbes (Nov. 30, 2011), https://www.forbes.com/sites/kashmirhill/2011/11/30/so-what-are-these-privacy-audits-that-google-and-facebook-have-to-do-for-the-next-20-years/#2cef17195000 [https://perma.cc/DC7Z-FM2P]; Smith, supra note 9 ("Since the early 2000s, our data security orders had contained fairly standard language. For example, these orders typically required a company to implement a comprehensive information security program subject to a biennial outside assessment.").

80. See Uber Technologies, Inc., FTC File No. 152-3054, 2018 WL 5631074, at *1 (F.T.C. Oct. 26, 2018) (statement of Commissioner Rebecca Kelly Slaughter) [hereinafter Slaughter Statement].

comply with a consent decree.[81] This benefits large corporations concerned about a decline in stock value from publicly available information about the corporation's data security compliance. But the lack of meaningful public assessments also benefits the FTC because the compliance efforts the agency pursues do not have to follow a uniform approach for each corporation under a consent order. A particularly revealing quote from one FTC Commissioner suggests the efforts of the Commission staff go far beyond what can be gleaned from any assessment:

> [A]ny privacy or data security assessment that is released to the public . . . will not provide a complete picture of a company's compliance under an FTC order, or the FTC's efforts in monitoring that company's compliance. This is . . . because *the FTC's compliance monitoring efforts in many cases extend far beyond what can be gleaned from an isolated assessment.*[82]

As a result, what the FTC considers "reasonable" data security measures is further hidden from public view. This provides additional support for the Eleventh Circuit's conclusion in *LabMD* that the FTC's data security consent orders require companies "to implement and maintain . . . data-security program[s] 'reasonably designed' to the Commission's satisfaction."[83] Such a requirement provides regulated parties not subject to FTC consent decrees little information about what the Commission considers appropriate data security, and may allow the Commission to regulate parties facing similar security threats differently. Given these problems with the FTC's current data security enforcement practice, the next Part discusses how regulated parties can be provided further notice of the FTC's data security requirements.

## III. CLARIFYING THE FTC'S DATA SECURITY ENFORCEMENT AUTHORITY

Despite the lack of clear data security standards creating uncertainty for businesses about whether there will be an enforcement action following a data breach, a solution to the problem has "confounded Congress."[84] This Part argues that there are two solutions to clarifying the FTC's data security standards, one that requires congressional action and another that can be achieved without congressional action. Section III.A proposes that,

---

81. See generally Megan Gray, Understanding and Improving Privacy "Audits" Under FTC Orders 4–8 (Apr. 18, 2018) (unpublished manuscript), http://cyberlaw.stanford.edu/files/blogs/white%20paper%204.18.18.pdf [https://perma.cc/VR7E-Y7FG] (explaining that the third-party assessments that the FTC requires when companies are under consent orders are "so vague or duplicative as to be meaningless" and often focus on the company's policies and not on the technical compliance).

82. See Slaughter Statement, supra note 80, at *1 (emphasis added).

83. See LabMD, Inc. v. FTC, 894 F.3d 1221, 1230 (11th Cir. 2018).

84. Neil Haggerty & Joe Adler, 6 Banking Issues to Watch when Congress Reconvenes, Am. Banker (Aug. 26, 2019), https://www.americanbanker.com/list/6-banking-issues-to-watch-when-congress-reconvenes [https://perma.cc/K7EZ-6RZD].

as part of the larger privacy bill being considered already, Congress adopt a private security standard as a *floor* for data security requirements and create a special exception to the FTC's burdensome rulemaking process specifically when more comprehensive data security regulations are necessary. Section III.B proposes that, with or without congressional action, regulated parties should begin commenting on FTC data security complaints, orders, and consent decrees to force the Commission to further specify what constitutes appropriate data security practices to avoid FTC enforcement actions.

### A. *Congress Should Adopt a Data Security Floor and Give the FTC Targeted Rulemaking Authority when Regulating Beyond the Floor Is Necessary*

Part of the problem with current FTC data security enforcement practice is that Congress has provided no guidance as to whether the FTC is even the appropriate agency to police data security practices, never mind particular standards outside of a few specific industries.[85] Now, the Commission has asked Congress for "comprehensive data security legislation . . . that would be enforced by the FTC."[86] Specifically, FTC Chairman Simons has asked for "targeted rule-making authority" in the data security context, governed by "clear and specific rules."[87] He has implored Congress to avoid "dump[ing] [the] question" of what rules to create on the FTC by granting the agency "broad rule-making authority."[88] Simons, an appointee of President Trump, is advocating the Republican position in the data security and privacy space, which seeks to avoid converting the FTC into "a massive rule-making regime"[89] and wants Congress to "create the rules, and the FTC . . . to enforce them."[90] Democrats, on the other hand, advocate giving the FTC increased rulemaking powers in both the data privacy and security contexts.[91]

This Comment proposes a middle ground to the disparate positions advocated by Democrats and Republicans in Congress. First, Congress should adopt one of the private data security standards set by various industry groups and other organizations as a *floor* for what constitutes "fair" data

85. For example, the security of healthcare data is regulated by the Health Insurance Portability and Accountability Act (HIPAA). 42 U.S.C. § 1320d-2 (2018).

86. Press Release, FTC, FTC Testifies Before Senate Commerce Subcommittee About the Agency's Work to Protect Consumers, Promote Competition, and Maximize Resources (Nov. 27, 2018), https://www.ftc.gov/news-events/press-releases/2018/11/ftc-testifies-senate-commerce-subcommittee-about-agencys-work [https://perma.cc/MY3U-PFGR].

87. See Bartz, supra note 8.

88. Id.

89. Id.

90. See Ben Lovejoy, Republican and Democrat Lawmakers Agree on the Need for Federal Privacy Law—But Not on Approach, 9to5Mac (May 9, 2019), https://9to5mac.com/2019/05/09/federal-privacy-law-2 [https://perma.cc/QKM7-F9JF].

91. Id.

security practices.[92] If a company is not following those standards, the FTC would have the ability to begin an enforcement action to force compliance. Second, Congress should provide the FTC with targeted rulemaking authority for either establishing more specific standards in individual industries that face unique data security challenges (and only those industries with unique challenges) or creating standards to respond to new cybersecurity threats faced by all data-holding industries. Importantly, the targeted rulemaking authority should be a specific data security exception to the FTC's burdensome Magnuson–Moss rulemaking procedures—which include requirements like an informal hearing where interested parties are entitled to present oral testimony and potentially cross-examine witnesses—and be guided by the Administrative Procedure Act.[93] While this would give the FTC more authority, it would also help clarify the requirements to regulated parties.

There are likely two primary objections to such an approach. The first objection would likely come from opponents of big business who would advocate that private standards are not as rigorous as those the FTC may adopt if given complete rulemaking authority for data security regulation. However, the FTC may not have the expertise, budget, or number of employees necessary to create the Commission's own standards. Currently, the Commission has only forty employees dedicated to data security enforcement,[94] which may be contributing to the current lack of clear enforcement standards. And the last time the federal government attempted to create cybersecurity standards—the Department of Commerce's voluntary National Institute of Standards and Technology (NIST) framework—the task force ended up adopting five separate sets of industry standards, each of which comprises only part of the seventy-two data security practices that can be found through examination of FTC data security actions.[95] Choosing one set of private industry standards would eliminate the complexity of

92. See Peter Cleveland, 10 Key Private-Sector Cybersecurity Standards, Enterprise IoT Insights (Sept. 24, 2018), http://enterpriseiotinsight.com/20180924/fundamentals/10-key-private-sector-cybersecurity-standards (on file with the *Columbia Law Review*) (including a comprehensive list of private cybersecurity standards, including one adopted by the FDA for medical devices); Jake Olcott, Cybersecurity Compliance: Regulations For 7 Industry Sectors, BitSight (Feb. 9, 2017), https://www.bitsight.com/blog/cybersecurity-compliance-regulations-for-7-industry-sectors [https://perma.cc/32YQ-X7HZ]; see also Insurance Data Security Model Law, Nat'l Ass'n of Ins. Commissioners (2017), https://www.naic.org/store/free/MDL-668.pdf [https://perma.cc/RX3F-YMJZ] (detailing the model data security requirements for insurance industry data); Maintaining Payment Security, PCI Sec. Standards Council, https://www.pcisecuritystandards.org/pci_security/maintaining_payment_security [https://perma.cc/X6FK-BHZW] (last visited Jan. 2, 2020) (describing payment security standards for merchants).

93. See Hartzog & Solove, Scope and Potential, supra note 74, at 2258 n.160.

94. Neidig, supra note 41.

95. See Manne & Stout, supra note 23, at 74.

establishing a floor and give the FTC the ability to focus on rulemaking in areas where more is needed as well as on enforcement.

The second objection would come from privacy advocates who have asked Congress to set up an entirely new data protection agency, contending that the FTC "has failed to enforce the orders it has established" and should be forced to focus on antitrust cases, not data security and privacy enforcement.[96] However, it is unlikely Congress will create such an agency,[97] so this Comment proposes clarifying the FTC's authority in this space rather than starting over.[98]

### B. *Regulated Parties Can Comment*

Given the current doubts that Congress will address data security in new data privacy legislation,[99] regulated parties should get the FTC to defend its settlements and consent orders on the record to add to the short list of available resources the FTC provides on its website to explain what it considers "fair" data security measures. One of the main problems with the FTC's current approach to data security enforcement is that the agency is rarely forced to explain what the agency considers "unfair" because companies settle right away.[100] This results in few well-reasoned decisions in which the FTC is forced to present why it undertakes an enforcement action.[101] However, there is an underutilized tool that forces the FTC to provide more information. When the Commission issues a proposed consent order, the order is placed in the Federal Register and permits a comment period of thirty days before it becomes final.[102] When the consent order does become final, the FTC posts replies to all of the comments received

---

96. Letter from Marc Rotenberg, President, Elec. Privacy Info. Ctr. & Caitriona Fitzgerald, Elec. Privacy Info. Ctr., to Roger Wicker, U.S. Senator, Chairman, U.S. Senate Comm. on Commerce, Sci., and Transport. & Maria Cantwell, U.S. Senator, Ranking Member, U.S. Senate Comm. on Commerce, Sci., and Transport. (Apr. 29, 2019), https://epic.org/testimony/congress/EPIC-SCOM-ConsumerPerspectives-Apr2019.pdf [https://perma.cc/5RRZ-FPML].

97. Luke Mullins, Is It Finally Time for a National Bureau of Privacy?, Washingtonian (Dec. 5, 2019), https://www.washingtonian.com/2019/12/05/finally-time-national-bureau-privacy-marc-rotenberg [https://perma.cc/7G65-LX2H] (noting a proposed "data-protection agency" faces "long odds" of being passed by Congress).

98. In addition, the FTC already has a staff of forty employees dedicated to data security enforcement, although it is likely that number would need to expand. Neidig, supra note 41.

99. See Kosseff, supra note 9.

100. See supra note 64 and accompanying text.

101. See supra text accompanying notes 65–66.

102. See, e.g., Press Release, FTC, Uber Agrees to Expanded Settlement with FTC Related to Privacy, Security Claims (Apr. 12, 2018), https://www.ftc.gov/news-events/press-releases/2018/04/uber-agrees-expanded-settlement-ftc-related-privacy-security [https://perma.cc/257D-6NUW] ("The FTC will publish a description of the consent agreement package in the Federal Register . . . . The agreement will be subject to public comment for 30 days . . . after which the Commission will decide whether to make the proposed consent order final.").

during that thirty-day window.[103] One possibility for receiving, and challenging, the FTC's reasoning and enforcement authority might be to get the agency talking more by commenting on these proposed consent orders. While the FTC may be measured in the language it uses, asking specific questions about what the Commission plans to do to enforce the order, for example, could be a way to better understand how the current enforcement practices work.

## CONCLUSION

For the past couple of decades, the FTC has increasingly sought to become America's chief data privacy and security enforcer despite its mission as an antitrust agency. The FTC has used the broad language in Section 5 of the FTC Act to garner expansive authority to bring enforcement proceedings for what the Commission deems "unfair" data security practices. This Comment shows that regulated parties lack adequate notice about what "fair" data security practices means. Now, after the Eleventh Circuit called the FTC's data security enforcement authority into question in *LabMD*, the FTC's authority in this space faces significant uncertainty. To clarify data security standards to regulated parties, Congress should provide clear authority to the FTC—as part of the larger privacy bill being discussed in Congress—using a private industry standard as the floor and enabling the FTC to regulate beyond that only when an industry faces a unique data security challenge or new cybersecurity threats necessitate further base expectations for all data-holding industries. Whether or not Congress enacts new data security legislation, regulated parties should begin commenting on FTC data security complaints, orders, and consent decrees to force the Commission to better articulate its data security requirements.

The core tenet of American administrative law is the prevention of arbitrary government. While no one disagrees with having better protections for consumer data, businesses large and small deserve to know the minimum data security requirements the FTC expects, if only to ensure that the FTC is exercising lawful authority and not arbitrary power.

---

103. See, e.g., TRENDnet Timeline, supra note 65 (including a link to "Letters to Commenters," where the FTC includes its responses to all the comments received during the comment period).