Notre Dame Law Review

Volume 94 | Issue 5 Article 13

7-2019

A Repeated Call for Omnibus Federal Cybersecurity Law

Carol Li
Notre Dame Law School

A REPEATED CALL FOR OMNIBUS FEDERAL CYBERSECURITY LAW

*Carol Li**

INTRODUCTION

In 2013, Target reported that the credit card and personally identifiable information of "as many as 110 million customers" had been compromised.[1] In 2014, Yahoo! announced that a "state-sponsored actor" had gained access to personal information of 500 million users that year, and "all 3 billion user accounts had been compromised" in a data breach that occurred in 2013.[2] Nine months into 2014, nearly 2000 cybersecurity incidents were confirmed, "compromis[ing] almost [one] [b]illion records worldwide."[3] In 2017, Equifax reported a data breach that exposed nearly 150 million consumers.[4] Between January 2017 and August 2018, "[a]t least 16 separate security breaches occurred at retailers," including Macy's, Sears, Delta Air Lines, Best Buy, Panera, and Whole Foods.[5] Even after its Cambridge Analytica scandal, Facebook reported in 2018 that "at least 50 million users' data were confirmed at risk after attackers exploited a vulnerability that allowed them

* Candidate for Juris Doctor, Notre Dame Law School, 2020. Bachelor of Arts in Political Science and Sociology, Northwestern University, 2013. I would like to thank Professor Veronica Root Martinez for her guidance, feedback, and mentorship, and my colleagues on the *Notre Dame Law Review* for their revisions and suggestions. All errors are my own.

1 Taylor Armerding, *The 18 Biggest Data Breaches of the 21st Century*, CSO (Dec. 20, 2018), https://www.csoonline.com/article/2130877/data-breach/the-biggest-data-breaches-of-the-21st-century.html.

2 *Id.*; Jonathan Stempel & Jim Finkle, *Yahoo Says All Three Billion Accounts Hacked in 2013 Data Theft*, REUTERS (Oct. 3, 2017), https://www.reuters.com/article/us-yahoo-cyber/yahoo-says-all-three-billion-accounts-hacked-in-2013-data-theft-idUSKCN1C82O1.

3 Francis J. Burke, Jr. & Steven M. Millendorf, Cybersecurity and Privacy Enforcement: A Roundup of 2014 Cases 10 (2015), https://www.americanbar.org/content/dam/aba/administrative/litigation/materials/2015/2015-corporate-cle/8b_2_cybersecurity_and_privacy_enforcement.pdf.

4 Steve Ragan, *Equifax Says Website Vulnerability Exposed 143 Million US Consumers*, CSO (Sept. 7, 2017), https://www.csoonline.com/article/3223229/security/equifax-says-website-vulnerability-exposed-143-million-us-consumers.html.

5 Dennis Green & Mary Hanbury, *If You Shopped at These 16 Stores in the Last Year, Your Data Might Have Been Stolen*, BUS. INSIDER (Aug. 22, 2018), https://www.businessinsider.com/data-breaches-2018-4.

access to personal data."[6] Worse yet, it was found that "[t]he vulnerability was introduced on the site in July 2017, but Facebook didn't know about it until" mid-September 2018.[7]

One need not be a cybersecurity expert to recognize that cyber risk is escalating: companies that many of us regularly use, trust, and rely on are falling to data hacks left and right. The number of "[r]ecent highly publicized data breaches have underscored the growing reality that attacks on private corporations constitute a national security issue."[8] According to industry experts: "today it is a matter of when, not if, a company's data will be breached."[9] The Ponemon Institute reported in 2018 that "[t]he risk of cyber extortion and data breaches will increase in frequency," but that "[d]espite the growing cyber threat, cybersecurity is not considered a strategic priority."[10] In 2018, the average expenditures required to address a data breach continued to increase, with the average total expenditure increasing to $3.86 million and the average cost for each lost or stolen record increasing to $148.[11] Living "in a world where every action we take can be observed, recorded, analyzed, and stored[,] . . . consumers want better consumer protections over personal data."[12]

In Part I, this Note discusses the concerning regularity of high-profile data breaches that have occurred within the United States' weak and patchwork landscape of cybersecurity law. Part II discusses the challenges companies face when attempting to comply with the current cybersecurity law, and why companies who are deemed compliant are still falling victim to hackers and data breaches. Part III makes a call for federal legislation to replace the current, inadequate, fragmented, and uneven landscape of cybersecurity law. Part IV discusses numerous factors and incentives to consider in creating an omnibus federal cybersecurity law. Finally, Part V offers some critiques to creating an omnibus law.

---

6 Sarah Perez & Zack Whittaker, *Everything You Need to Know About Facebook's Data Breach Affecting 50M Users*, TECHCRUNCH (Sept. 28, 2018), https://techcrunch.com/2018/09/28 /everything-you-need-to-know-about-facebooks-data-breach-affecting-50m-users/.

7 *Id.*

8 Thad A. Davis et al., *The Data Security Governance Conundrum: Practical Solutions and Best Practices for the Boardroom and the C-Suite*, 2015 COLUM. BUS. L. REV. 613, 624.

9 David C. Grossman, *Blaming the Victim: How FTC Data Security Enforcement Actions Make Companies and Consumers More Vulnerable to Hackers*, 23 GEO. MASON L. REV. 1283, 1284 (2016); *see also* Scot Ganow & Zachary Heck, *Proactive Approach to Cybersecurity Pays Off in Ohio with New Data Protection Act*, TAFT: PRIVACY & DATA SECURITY INSIGHT (Aug. 13, 2018), https://www.privacyanddatasecurityinsight.com/2018/08/proactive-approach-to-cybersecurity-pays-off-in-ohio-with-new-data-protection-act/.

10 PONEMON INST., 2018 STUDY ON GLOBAL MEGATRENDS IN CYBERSECURITY 1–2 (2018), https://www.raytheon.com/sites/default/files/2018-02/2018_Global_Cyber_Megatrends.pdf.

11 PONEMON INST., 2018 COST OF A DATA BREACH STUDY: GLOBAL OVERVIEW 3 (2018), https://databreachcalculator.mybluemix.net/assets/2018_Global_Cost_of_a_Data_Breach_Report.pdf [hereinafter COST OF A DATA BREACH STUDY].

12 Justin Brookman, *Protecting Privacy in an Era of Weakening Regulation*, 9 HARV. L. & POL'Y REV. 355, 355 (2015).

I. Current State of Cybersecurity Law in the United States: A Fragmented Framework of Cybersecurity Obligations

Despite the increasing frequency of data privacy breaches compared to the rest of the world, "the legal framework to protect privacy and personal data in the United States is quite weak."[13] Part of this weakness is due to the fragmented, patchwork nature of cybersecurity laws, which in turn makes it difficult for companies to comply. As it stands, "[t]he United States does not have a national law that prescribes specific data security standards for all industries."[14] Instead, companies must figure out how to comply with a "fragmented and disconnected framework of state and federal laws governing cybersecurity obligations."[15] The United States' framework consists of "hundreds of state and federal statutes, regulations, binding guidelines, and court-created rules regarding data security, privacy, and other issues commonly considered to fall under the umbrella 'cybersecurity.'"[16] Once a breach occurs, "[c]ompanies . . . might face potential enforcement and private civil actions brought by" the Federal Trade Commission (FTC), the Securities and Exchange Commission (SEC), state attorneys general, the Department of Justice (DOJ), plaintiffs whose data was compromised, shareholders of the company, the Consumer Financial Protection Bureau, the Federal Communications Commission, and the Department of Health and Human Services, to name a few.[17] Facebook's Cambridge Analytica scandal spurred "investigations by four federal agencies"—the FBI, the FTC, the SEC, and the DOJ.[18]

A. Federal Sectoral Approach

While many other industrialized nations "protect all personal data in an omnibus fashion, privacy law in the United States is sectoral, with different laws regulating different industries and economic sectors."[19] The only federal data security laws that exist in the United States are industry specific, only "apply[ing] to companies that handle specific types of data, such as financial information or health records."[20] For example, "[t]here is a law for

13 *Id.* at 356.

14 Jeff Kosseff, Cybersecurity Law 1 (2017).

15 Jennifer Gordon, Note, *Like A Bad Neighbor, Hackers Are There: The Need for Data Security Legislation and Cyber Insurance in Light of Increasing FTC Enforcement Actions*, 11 Brook. J. Corp. Fin. & Com. L. 183, 185 (2016).

16 Kosseff, *supra* note 14, at xxi.

17 Judith H. Germano & Zachary K. Goldman, After the Breach: Cybersecurity Liability Risk 1 (2014), https://www.lawandsecurity.org/wp-content/uploads/2014/06/CLS-After-the-Breach-Final.pdf.

18 Sissi Cao, *Facebook Fined $660K for Cambridge Analytica, but Expert Says $7B More Is Underway*, Observer (July 11, 2018), https://observer.com/2018/07/uk-regulators-fined-facebook-660k-over-cambridge-analytica/.

19 Daniel J. Solove & Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, 114 Colum. L. Rev. 583, 587 (2014).

20 Kosseff, *supra* note 14, at 1.

video records and a different law for cable records."[21] And even within a particular sector, the federal law may not govern the entirety of data privacy within that industry. While the Health Insurance Portability and Accountability Act (HIPAA) of 1996 is federal legislation protecting the privacy and security of health information,[22] "[n]ot all health data is covered by HIPAA, and various constitutional and state laws can protect health data more stringently than HIPAA."[23] The federal sectoral approach results in fragmentation that "leaves large areas unregulated . . . at the federal level."[24] Without "a national law that prescribes specific data security standards for all industries,"[25] data collection by companies like Facebook, Google, and Amazon will remain ungoverned by federal law.[26]

B. Federal Trade Commission

The FTC has been the most prominent federal agency to enforce cybersecurity practices over the past two decades. This Note will focus on the growth, limitations, and criticisms of the FTC's enforcement authority in the cybersecurity area. Because of the gaps that are left in the sectoral data privacy laws at the federal level, "many companies fall outside of specific sectoral privacy laws."[27] The FTC has stepped in to enforce within those gaps. The FTC's privacy jurisprudence "has become 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."[28] Thus, "[t]he FTC is the closest thing that the U.S. federal government has to a centralized data security regulator."[29]

1. History of the FTC

The FTC was created in 1914 "to prevent unfair methods of competition in commerce as part of the battle to 'bust the trusts.'"[30] The FTC has the

21 Solove & Hartzog, *supra* note 19, at 587 (first citing Video Privacy Protection Act of 1988, 18 U.S.C. §§ 2710–2711 (2012); and then citing 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.)).

22 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. Code).

23 Solove & Hartzog, *supra* note 19, at 587.

24 *Id.*

25 KOSSEFF, *supra* note 14, at 1.

26 *See* Solove & Hartzog, *supra* note 19, at 587.

27 *Id.* at 588.

28 *Id.* at 585–86.

29 KOSSEFF, *supra* note 14, at 2. There are other agencies, such as the Department of Health and Human Services or the Federal Communications Commission, that have some jurisdiction to regulate data privacy and security, but they are limited to only particular sectors. *Id.*

30 *About the FTC*, FED. TRADE COMM'N, https://www.ftc.gov/about-ftc (last visited Feb. 25, 2019).

power to enforce "three targeted laws that oblige certain types of businesses to act reasonably in protecting consumer data."[31] However, for most of its privacy-related work, the FTC relies on its general authority under section 5(a)(1) of the Federal Trade Commission Act (FTCA)[32] to proscribe unfair or deceptive acts or practices.[33] This authority was given to the FTC when Congress passed the Wheeler-Lea Amendment in 1938, which included "a broad prohibition against 'unfair and deceptive acts or practices.'"[34]

"Despite the lack of a statute that sets minimum data security requirements, the Federal Trade Commission aggressively polices data security."[35] For the many companies that "fall outside of specific sectoral privacy laws, the FTC is in many cases the primary source of regulation."[36] The FTC has used FTCA section 5 to bring complaints against companies that violate their consumers' privacy rights or fail to meet the guarantees of their privacy policies.[37]

In 1995, when "the FTC became involved with consumer privacy issues[,] . . . [i]nstead of the FTC creating rules, the companies themselves would create their own rules, and the FTC would enforce them. . . . The FTC thus would serve as the backstop to the self-regulatory regime, providing it with oversight and enforcement . . . ."[38] To start, the FTC policed privacy policies "by focusing on deceptive trade practices."[39] "Prior to 1964, the [FTC] largely ignored the word 'or' in [FTCA section 5]," making little "attempt to distinguish between 'unfair' . . . and 'deceptive.'"[40] However, FTCA section 5 "gives the FTC two different tests for an organization's data

31 Alden F. Abbott, *The Federal Trade Commission's Role in Online Security: Data Protector or Dictator?*, Heritage Found. (Sept. 10, 2014), http://thf_media.s3.amazonaws.com/2014/pdf/LM137.pdf [hereinafter Abbott, *The Federal Trade Commission*] ("The commission's Safeguards Rule, which it adopted pursuant to the Gramm-Leach-Bliley Act, sets forth data security requirements for non-bank financial institutions. The Fair Credit Reporting Act (FCRA) requires that consumer reporting agencies use reasonable precautions to ensure that the entities to which they disclose sensitive consumer information have a permissible scope for receiving that information and imposes safe disposal obligations on entities that maintain consumer report information. The Children's Online Privacy Protection Act (COPPA) requires reasonable security measures to safeguard children's information collected online." (footnotes omitted)).

32 Federal Trade Commission Act § 5(a)(1), 15 U.S.C. § 45(a) (2012)).

33 Abbott, *The Federal Trade Commission*, *supra* note 31.

34 *About the FTC*, *supra* note 30; *see also* Solove & Hartzog, *supra* note 19, at 598.

35 Kosseff, *supra* note 14, at 1.

36 Solove & Hartzog, *supra* note 19, at 588.

37 *See, e.g.*, *id.* at 628–30.

38 *Id.* at 598 (footnote omitted).

39 *Id.* at 599.

40 J. Howard Beales, *The FTC's Use of Unfairness Authority: Its Rise, Fall, and Resurrection*, Fed. Trade Commission (May 30, 2003) (quoting Federal Trade Commission Act, ch. 49, 52 Stat. 111 (codified as amended at 15 U.S.C. § 45(a) (2012)), https://www.ftc.gov/public-statements/2003/05/ftcs-use-unfairness-authority-its-rise-fall-and-resurrection.

privacy and cybersecurity practices."[41] The FTC uses the "deceptive" prong under FTCA section 5 to bring data privacy enforcement actions "[i]f an organization holds itself out as having implemented a certain data privacy practice . . . [and] act[s] outside that data privacy practice."[42] Thus, "[w]hile the United States doesn't have strong privacy rules like the [General Data Protection Regulation], the FTC has a rule that organizations must abide by their own privacy policies, and it can take action against those that fail to do so."[43]

The FTC uses the "unfair" prong under FTCA section 5 "to bring actions against entities with known data breaches," under the logic that "[l]ax cybersecurity . . . is an unfair method of competition."[44] Today, the FTC applies a three-part test, which is codified in FTCA section 5(n), to determine whether a practice is "unfair": "[T]o warrant a finding of unfairness, an injury '[1] must be substantial; [2] it must not be outweighed by any countervailing benefits to consumers or competition that the practice produces; and [3] it must be an injury that consumers themselves could not reasonably have avoided.'"[45] Before *FTC v. Wyndham Worldwide Corp.*,[46] "the FTC focused primarily on the deception prong of Section 5 to trip up companies that failed to live up to statements they made about their data use and security practices."[47]

Instead of defining or listing which specific practices would constitute unfairness, "Congress 'intentionally left development of the term "unfair" to the Commission' through case-by-case litigation."[48] Additionally, "[t]he Commission is authorized under 15 U.S.C. § 57a to prescribe rules 'which define with specificity' unfair acts or practices within the meaning of Section 5(a)."[49] Once a rule is defined, "it becomes in essence an addendum to Section 5(a)'s phrase 'unfair . . . acts or practices' [and] the rule puts the public on notice that a particular act or practice is unfair."[50] In the case-by-case litigation context, "once an act or practice is adjudged to be unfair, the act or

41 John McCauley & Kyle Miller, LabMD *and the Future of FTC Data Privacy Regulation*, BINGHAM GREENEBAUM DOLL (July 17, 2018), https://www.bgdlegal.com/blog/labmd-and-the-future-of-ftc-data.

42 *Id.*

43 Grant Gross, *How Updated Privacy Policies Could Make GDPR the Global Standard*, PARALLAX (May 25, 2018) (citation omitted), https://www.the-parallax.com/2018/05/25/ftc-gdpr-privacy-standard/.

44 McCauley & Miller, *supra* note 41.

45 LabMD, Inc. v. FTC, 894 F.3d 1221, 1229 (11th Cir. 2018) (quoting *FTC Policy Statement on Unfairness*, FED. TRADE COMM'N (Dec. 17, 1980), https://www.ftc.gov/public-statements/1980/12/ftc-policy-statement-unfairness (alterations in original)).

46 799 F.3d 236 (3d Cir. 2015).

47 Allison Grande, *Landmark FTC Win Fuels Uncertainty for Data Breach Targets*, LAW360 (Apr. 8, 2014), https://advance.lexis.com/api/permalink/e153167e-28ca-4d31-89c7-dcbfc9daa643/?context=1000516.

48 *LabMD*, 894 F.3d at 1228 (quoting Atl. Ref. Co. v. FTC, 381 U.S. 357, 367 (1965)).

49 *Id.* at 1231 (quoting 15 U.S.C. § 57a(a)(1)(B) (2012)).

50 *Id.* (omission in original) (quoting Federal Trade Commission Act § 5(a), 15 U.S.C. § 45(a) (2012)).

practice becomes in effect—like an FTC-promulgated rule—an addendum to Section 5(a)."[51] However, in the vast majority of enforcement actions that the FTC brings against companies, "nearly all [FTC actions] end[ ] in settlements rather than case law."[52]

2. FTC Enforcement Actions and Development of a "Jurisprudence of Privacy"

Since 2006, the FTC "has held businesses responsible for their privacy and security promises to consumers under its power to investigate unfair and deceptive trade practices granted in Section 5 of the Federal Trade Commission Act."[53] "[T]he FTC has brought dozens of enforcement actions against companies that it believes have failed to take reasonable steps to secure the personal data of their customers."[54] FTCA section 5 is "a century-old law that was designed to protect consumers and competitors from unfair business practices."[55] If the FTC determines that a company is engaging in inadequate cybersecurity practices, the FTC will threaten to file a lawsuit under FTCA section 5.[56] Instead of proceeding to trial, most companies agree to a consent order, which "generally require companies to develop comprehensive information security programs, obtain periodic independent assessments of their information security, and provide the FTC with broad oversight and access into the company's programs for up to twenty years."[57] Violating the consent order "can result in significant fines," but agreeing to a consent order allows a company to avoid admission of guilt, the risks of publicity, and the costs of litigation.[58]

The FTC has not consistently gone after repeat offenders, leading to a "questionable track record of holding companies accountable for privacy violations."[59] Without holding repeat offenders accountable, the FTC undermines "the credibility of law enforcement and regulatory agencies . . . by the real or perceived lax treatment of repeat offenders."[60] For example, Facebook has been under a consent decree since 2011, but has since been embroiled in the Cambridge Analytica scandal.[61] The FTC announced in March 2018 that it "takes very seriously recent press reports raising substan-

51 *Id.* at 1232.

52 Solove & Hartzog, *supra* note 19, at 588.

53 Burke & Millendorf, *supra* note 3, at 3.

54 Kosseff, *supra* note 14, at 1.

55 *Id.*

56 *Id.* at 5–6.

57 *Id.* at 6.

58 *Id.*

59 Gross, *supra* note 43.

60 Jesse Eisinger, *New Commissioner Says FTC Should Get Tough on Companies Like Facebook and Google*, ProPublica (May 14, 2018), https://www.propublica.org/article/rohit-chopra-ftc-commissioner-ftc-should-get-tough-on-companies-like-facebook-and-google.

61 *See* Tony Romm & Craig Timberg, *FTC Opens Investigation into Facebook After Cambridge Analytica Scrapes Millions of Users' Personal Information*, Wash. Post (Mar. 20, 2018), https://www.washingtonpost.com/news/the-switch/wp/2018/03/20/ftc-opens-investiga

tial concerns about the privacy practices of Facebook . . . [and] confirm[ed] that it has an open non-public investigation into these practices."[62]

FTC consent orders generally last twenty years; the timespan may make the orders unnecessarily expensive and create unintended problems for companies.[63] First, twenty years of FTC oversight is a costly task—for an Agency already short on time and resources, twenty years is far too long. More significantly, if the past twenty years are any indication, "changes in technology, consumer expectations, and the marketplace" will likely be substantial over a twenty-year period.[64] In 2017, Sears Holdings Management Corporation ("Sears") submitted a petition to the FTC "to reopen and modify the settlement to which they agreed in 2009."[65] In its petition, Sears argued that the 2009 consent order required it to "handl[e] consumer notices in its mobile applications in a way different from other companies' industry-standard mobile apps" in a way that did not align with consumer's changing expectations.[66] Sears additionally argued that compliance with the consent order "imposed 'heavy' competitive burdens that 'significantly disadvantaged Sears in the marketplace.'"[67] With the changing commercial landscape, "[m]any companies will not be doing business in 20 years . . . [and] [e]ven large Fortune 500 companies significantly change in a decade."[68] Additionally, the prescriptive requirements in FTC consent orders "may . . . become obsolete, given changes in the market" over the twenty-year life of the order.[69] If the FTC is unwilling to modify its 2009 consent order that actually "harm[s] Sears' ability to compete in the marketplace[,] . . . Sears will need to continue to comply with the arguably antiquated requirements for another 12 years."[70]

3. Expansion of FTC Authority After *Wyndham Worldwide*

One of the first companies to "mount a serious challenge to the FTC's cybersecurity enforcement authority" was Wyndham Worldwide Corpora-

---

tion-into-facebook-after-cambridge-analytica-scrapes-millions-of-users-personal-information/?utm_term=.cf4ca66ec032.

62 Press Release, Fed. Trade Comm'n, Statement by the Acting Director of FTC's Bureau of Consumer Protection Regarding Reported Concerns About Facebook Privacy Practices (Mar. 26, 2018), https://www.ftc.gov/news-events/press-releases/2018/03/statement-acting-director-ftcs-bureau-consumer-protection.

63 *See* KOSSEFF, *supra* note 14, at 5–6.

64 Wendell Bartnick, *Sears Petitions to Change Its 8-Year-Old FTC Privacy Settlement Order*, REEDSMITH (Dec. 4, 2017), https://www.technologylawdispatch.com/2017/12/cookies-tracking-online-behavioral-advertising/sears-petitions-to-change-its-8-year-old-ftc-privacy-settlement-order/.

65 *Id.*

66 *Id.*

67 *Id.*

68 *Id.*

69 *Id.*

70 *Id.*

tion.[71] Instead of agreeing to a consent order, as most companies do when faced with the threat of a lawsuit by the FTC, "Wyndham moved to dismiss the lawsuit, arguing . . . that Section 5 does not provide the FTC with the authority to bring cybersecurity-related actions against companies."[72]

In *FTC v. Wyndham Worldwide Corp.*,[73] the Third Circuit held that a company's failure to maintain reasonable and appropriate data security could constitute unfair commercial competition practices.[74] Additionally, the court noted that subsequent congressional acts did not preclude FTCA section 5 from covering cybersecurity issues.[75] The decision in *Wyndham Worldwide* was seen as a huge victory for the FTC, as the decision affirmed the Agency's "broadened . . . focus to encompass companies that it claims have violated Section 5's unfairness prong by failing to adequately protect consumer data from unauthorized disclosure or misuse."[76] After *Wyndham Worldwide*, the FTC has the authority to take action against bad security practices. Despite the fact that "Congress has not passed a statute that provides the FTC with general authority to regulate cybersecurity,"[77] and even though the court's ruling in *Wyndham Worldwide* is only binding in the Third Circuit, "it is largely accepted that the FTC has some authority to bring Section 5 complaints against companies that fail to adequately secure customer data."[78]

4. The Limits of the FTC's Sanctioning Authority

Notably, the FTC's ability to impose sanctions on companies is restricted in scope and severity. The FTC is only able to "enforce FTC Act violations or infringements of other laws that granted it regulatory authority."[79] The FTC "lack[s] the ability to enact substantive privacy rules of its own,"[80] and if the company does not fall within the scope of another privacy policy that provides the FTC authority, "then the FTC would have nothing to enforce."[81] Thus, the FTC's sanctioning authority is "limited to . . . whatever a company promised."[82] In 2012, "the FTC issued a $22.5 million dollar fine" against Google, which was noted as "a small drop in the bucket" of Google's $37.9 billion in revenue the previous year.[83] As will be discussed in subsection

71 KOSSEFF, *supra* note 14, at 6.
72 *Id.*
73 799 F.3d 236 (3d Cir. 2015).
74 *Id.* at 249.
75 *Id.* at 248.
76 Grande, *supra* note 47.
77 KOSSEFF, *supra* note 14, at 5–6.
78 *Id.* at 2.
79 Solove & Hartzog, *supra* note 19, at 599.
80 *Id.* Congress, over the years, *has* given the FTC rulemaking and enforcement authorities, but they are limited to specific privacy laws, such as COPPA. *See id.* at 602–03.
81 *Id.* at 599.
82 *Id.*
83 *Id.* at 605–06.

I.C.2, while the General Data Protection Regulation (GDPR) may increase compliance requirements for some companies, the FTC's ability to enforce the GDPR within the United States is limited to companies that (1) decide to implement the GDPR within its operations, and (2) violate that privacy promise.[84]

The severity of the FTC's penalties is also quite limited. "[I]n most cases, the FTC cannot levy a fine against a company that violates its own privacy promises."[85] Once the FTC brings an enforcement action against a company and that company agrees to a consent order—which generally "requires the targeted company to create a comprehensive privacy or security plan, and to submit to independent audits every other year for 20 years"—only "[i]f the company . . . violates the agency enforcement plan[ ] [can] the FTC . . . levy fines of more than $40,000 per violation."[86] However, "any fines issued by the FTC must reflect the amount of consumer loss."[87] The average cost per lost or stolen record, however, is estimated to be $148.[88] When the FTC does fine a company, the fines "are often quite small in relation to the gravity of the violations and the overall net profit of the violators."[89]

5. The FTC's Body of "Law"

While the FTC may have some authority to take action against bad data security practices as a result of *Wyndham Worldwide*, its use of "a patchwork of consent decrees and informal statements is insufficient" if it wants to "shape[ ] industry norms and legal standards—if it wants to develop a general law of data security."[90] What is currently missing from the FTC's enforcement process are "decision[s] on the merits" and the development of "legally binding rules through . . . rulemaking procedures."[91] In a footnote, the *Wyndham Worldwide* court "agree[s] with Wyndham that the consent orders, which admit no liability and which focus on prospective requirements on the defendant, [are] of little use to [businesses] in trying to understand the specific requirements imposed by [FTCA section 5(a)]."[92] The Third Circuit went on to recognize that it "may be unfair to expect private parties . . . to have examined FTC complaints or consent decrees."[93] While the Commission offered no examples of it "inform[ing] the public that it needs

84 *See* Gross, *supra* note 43.

85 *Id.*

86 *Id.*

87 Solove & Hartzog, *supra* note 19, at 605.

88 COST OF A DATA BREACH STUDY, *supra* note 11, at 3.

89 Solove & Hartzog, *supra* note 19, at 605.

90 Gus Hurwitz, *In* Wyndham*, the FTC Won a Battle but Perhaps Lost Its Data Security War*, AEIDEAS (Aug. 27, 2015), http://www.aei.org/publication/wyndham-ftc-won-battle-perhaps-lost-data-security-war/.

91 *Id.*

92 FTC v. Wyndham Worldwide Corp., 799 F.3d 236, 257 n.22 (3d Cir. 2015).

93 *Id.* at 257 n.23.

to look at complaints and consent decrees for guidance," it still argued that a "careful general counsel [would] pay attention to what the FTC is doing."[94]

In some instances, the FTC has published recommendations "without inquiring into whether such onerous new requirements would prove cost-beneficial to producers or to consumers."[95] In 2014, the FTC recommended a set of limitations in the data broker area to Congress, without first undergoing "a serious empirical analysis of consumer harm in this area."[96] Commissioner Joshua Wright spoke to the problematic nature of the FTC's recommendations, stating that the FTC cannot issue recommendations and guidance without a thorough analysis of how the costs to businesses might affect consumers.[97] Without enough research and analysis, the FTC's questionable recommendations may actually "reduce consumer welfare."[98]

Additionally, the FTC's enforcement of FTCA section 5 will be tied to who sits on the Commission. The FTC consists of five commissioners, "nominated by the President and confirmed by the Senate, each serving a seven-year term."[99] Thus, acting without formal guidelines, the FTC's enforcement of FTCA section 5 "can be as broad or as narrow as a majority of the commissioners at any given time believe it to be, and the business community suffers from the resulting uncertainty."[100] Though Professors Daniel Solove and Woodrow Hartzog argue that the "FTC's privacy jurisprudence is quite thick," with standards resembling rules,[101] former Commissioner Joshua Wright recognized that the "common-law, case-by-case approach to defining Section 5 . . . is undesirable because it leads to inconsistent and unpredictable results, and invites Congress and the courts to step in and define the FTC's authority."[102]

The authority of the FTC may also be at the mercy of court decisions. In *LabMD v. FTC*, the Eleventh Circuit criticized the FTC for overreaching, because its "order contain[ed] no prohibitions."[103] Instead of "instruct[ing] LabMD to stop committing a specific act or practice . . . [the order] command[ed] LabMD to overhaul and replace its data-security program to meet an indeterminable standard of reasonableness."[104] The mandate of "a complete overhaul of LabMD's data-security program" was held unenforceable

94 *Id.*

95 Abbott, *The Federal Trade Commission*, *supra* note 31, at 8.

96 *Id.*

97 *Id.*

98 *Id.* at 10.

99 *Commissioners*, FED. TRADE COMM'N, https://www.ftc.gov/about-ftc/commissioners (last visited Nov. 25, 2018).

100 BAKERHOSTETLER, THE PAST, PRESENT, AND FUTURE OF SECTION 5 OF THE FTC ACT: PERSPECTIVES FROM THE COMMISSION, THE JUDICIARY, AND CONGRESS (2015), https://www.bakerlaw.com/files/uploads/Documents/News/Articles/LITIGATION/2015/Past-Present-Future-Section%205-White-Paper.pdf.

101 Solove & Hartzog, *supra* note 19, at 586.

102 BAKERHOSTETLER, *supra* note 100.

103 LabMD, Inc., v. FTC, 894 F.3d 1221, 1236 (11th Cir. 2018).

104 *Id.*

because the Commission said "precious little about how this [was] to be accomplished[,] . . . effectually charg[ing] the district court with managing the overhaul."[105] Based on this ruling, the FTC will likely "have to tailor the conditions it imposes on companies it has accused of failing to safeguard consumer data" by "set[ting] specific data security benchmarks for corporate defendants."[106] This ruling and rebuke of the FTC for overreaching "means confusion, nervousness, new challenges to the FTC's authority and the need to develop new and improved compliance orders."[107] If *LabMD* stands, "it could affect the viability of some of the Commission's remedial powers," including some of the already-existing consent orders that "include[ ] broad prophylactic remedies that are similarly premised on a reasonableness standard."[108]

Thus, the "FTC's self-styled 'common-law' approach to data security regulation is yielding an unsound body of law."[109] Despite over fifteen years of FTC enforcement, there is no meaningful body of judicial decisions to show for it. Nearly all cases have resulted in settlement agreements.[110] While consent orders may be lengthy and inconvenient, "there is considerable evidence that consent orders 'lack teeth,' permitting companies tremendous flexibility to satisfy the terms of the consent order without improving privacy and security practices internally."[111] Thus, companies live in a world where the FTC has broad authority to take action against companies for their data security practices, but its ability to issue clear guidance on what constitutes bad data security practices is convoluted and unclear.

C. Global Pressures

1. European Union's General Data Protection Regulation

In 2016, the European Union passed the General Data Protection Regulation (GDPR)[112] as its "omnibus data protection law," replacing the Euro-

105 *Id.* at 1237.

106 Alison Frankel, *There's a Big Problem for the FTC Lurking in 11th Circuit's* LabMD *Data-Security Ruling*, REUTERS (June 7, 2018), https://www.reuters.com/article/us-otc-labmd/theres-a-big-problem-for-the-ftc-lurking-in-11th-circuits-labmd-data-security-ruling-idUSKCN1J32S2.

107 Kirk Nahra, *Takeaways from the 11th Circuit* FTC v. LabMD *Decision*, IAPP (June 7, 2018), https://iapp.org/news/a/takeaways-from-the-11th-circuit-ftc-vs-labmd-decision/.

108 Rafael Reyneri, *Eleventh Circuit* LabMD *Decision Potentially Limits FTC's Remedial Powers*, COVINGTON: INSIDE PRIVACY (June 11, 2018), https://www.insideprivacy.com/united-states/federal-trade-commission/eleventh-circuit-labmd-decision-potentially-limits-ftcs-remedial-powers/.

109 Justin (Gus) Hurwitz, *Data Security and the FTC's UnCommon Law*, 101 IOWA L. REV. 955, 955 (2016).

110 *See* Solove & Hartzog, *supra* note 19, at 585.

111 Michelle De Mooy, *How to Strengthen the FTC Privacy & Security Consent Decrees*, CTR. FOR DEMOCRACY & TECH. (Apr. 12, 2018), https://cdt.org/blog/how-to-strengthen-the-ftc-privacy-security-consent-decrees/.

112 *See* Commission Regulation 2016/679, 2016 O.J. (L 119) (EU) [hereinafter GDPR].

pean Union's twenty-year-old Data Protection Directive.[113] The Data Protection Directive was issued in 1995, during a very different technology era than today.[114] Additionally, the Data Protection Directive "was limited because it was just that—a directive."[115] The Data Protection Directive set a minimum baseline that "EU member states had to meet in their own data protection laws," but each member state "could craft their own laws as they saw fit."[116] Similar to the current state of cybersecurity law in the United States, the Directive model "led to a patchwork of data protection laws across Europe, with some countries implementing more stringent (and occasionally more unique) laws than others."[117] By passing the GDPR, the European Union "directly impose[d] a uniform data security law regime on all EU members . . . thereby harmonizing EU data protection law."[118]

The GDPR, comprised of ninety-nine articles over 261 pages, "set[s] out the rights of individuals and obligations placed on businesses that are subject to the regulation."[119] Notably, the GDPR provides data subjects with greater control.[120] The GDPR mandates that companies receive consumer consent, defined as a "clear affirmative act establishing a freely given, specific, informed and unambiguous indication of the data subject's agreement to the processing of personal data."[121] The "[r]ight to data portability" allows data subjects to request any personal data a company has on them and "transmit [their] data to another controller without hindrance."[122] Additionally, data subjects have the "[r]ight to erasure" or the "right to be forgotten," and in certain situations, "the controller shall have the obligation to erase personal data without undue delay."[123] The GDPR also requires that companies appoint and hire a data protection officer.[124] Data protection officers are tasked with "inform[ing] and advis[ing] the controller or the processor," "monitor[ing] compliance with [the GDPR]," "provid[ing] advice where requested . . . and monitor[ing] its performance," and "cooperat[ing] with the supervisory authority."[125] Additionally, "any data that can be used to

113 Courtney M. Bowman, *A Primer on the GDPR: What You Need to Know*, PROSKAUER: PRIVACY L. BLOG (Dec. 23, 2015), https://privacylaw.proskauer.com/2015/12/articles/european-union/a-primer-on-the-gdpr-what-you-need-to-know/.

114 *See id.*

115 *Id.*

116 *Id.*

117 *Id.*

118 *Id.*

119 Andrew Rossow, *The Birth of GDPR: What Is It and What You Need to Know*, FORBES (May 25, 2018), https://www.forbes.com/sites/andrewrossow/2018/05/25/the-birth-of-gdpr-what-is-it-and-what-you-need-to-know/#1d18f7955e5b.

120 *See* GDPR, *supra* note 112, arts. 12–16, at 39–43 (describing the rights of the data subject).

121 *Id.* at 6.

122 *Id.* art. 20, at 45.

123 *Id.* art. 17, at 43–44.

124 Rossow, *supra* note 119.

125 GDPR, *supra* note 112, art. 39, at 56.

identify an individual—be it genetic, psychological, cultural, religious and/or socioeconomic—all now falls under the GDPR umbrella."[126]

The GDPR affects European Union member states and applies not just to European businesses, but additionally "to any entities that work with [European] businesses as well, thus making GDPR a global data protection law."[127] Companies who are within the scope of the GDPR and are noncompliant with it may face astronomical penalties, with fines up to four percent of total worldwide annual turnover or twenty million euros, whichever is higher.[128]

2. FTC's Enforcement of the GDPR

On top of attempting to understand and comply with the GDPR, the FTC has also signaled that it plans to enforce statements of GDPR compliance. Three U.S. companies have already agreed to settle FTC charges that they misled consumers about their participation in the European Union–United States Privacy Shield framework.[129] Since FTCA section 5 authorizes FTC actions for "deceptive practices," its enforcement creates incentives for companies to *not* make promises to be GDPR compliant. Instead, "[a]s companies revamp their privacy policies to comply with the GDPR, many have been careful to avoid making new promises."[130] This is an example of the problematic incentive created by the FTC in how it enforces companies' privacy policies: companies will simply be careful to not overpromise their security measures so as to escape scrutiny by the FTC. This *dis*incentive is at odds with how we want companies to operate—we *want* to encourage companies to increase their cybersecurity practices.

3. GDPR-Inspired Legislation in Brazil and India

Business executives believe that "the GDPR will likely inspire other countries to expand data privacy regulations."[131] Since the GDPR was adopted, Brazil and India have followed suit with GDPR-inspired data laws.[132] In July

126 Manuel Grenacher, *GDPR, The Checklist for Compliance*, FORBES (June 4, 2018), https://www.forbes.com/sites/forbestechcouncil/2018/06/04/gdpr-the-checklist-for-compliance/.

127 *Id.*

128 *See* GDPR, *supra* note 118, art. 83, at 82–83.

129 *See* Katherine E. Armstrong, *The FTC's First Privacy Shield Enforcement Actions*, LEXOLOGY (Sept. 11, 2017), https://www.lexology.com/library/detail.aspx?g=7610e1ea-ca11-497f-9ebb-2e1ee09b5d13.

130 Gross, *supra* note 43.

131 Ross Benes, *Business Execs Believe More Countries Will Adopt GDPR-Like Laws*, EMARKETER (Oct. 25, 2018), https://www.emarketer.com/content/business-execs-believe-more-countries-will-adopt-gdpr-like-laws.

132 *See* Jessica Trevellick, *New GDPR-Inspired Data Laws in Brazil and India*, JDSUPRA (Aug. 27, 2018), https://www.jdsupra.com/legalnews/new-gdpr-inspired-data-laws-in-brazil-95445/.

2018, India published a first draft of its new Personal Data Protection Bill.[133] In August 2018, Brazil's President signed the "lei geral de proteção de dados pessoais," which will go into effect in February 2020.[134] Notably, the rules contained in both Brazil's and India's new data privacy legislation "will be applicable not only to companies based in Brazil and India but also to businesses outside of those countries that are processing the personal data of Brazilian and Indian citizens."[135] Just as the GDPR requirements extend to non-EU organizations that deal with EU citizens, the Brazil and India requirements will similarly extend to organizations that deal with the personal data of their citizens. Thus, U.S. companies must also consider the cybersecurity requirements of a growing number of other countries.

D. State Law and State Enforcement

An additional layer to federal sectoral data privacy laws is that "most state privacy laws are sectoral as well,"[136] which further complicates what companies must comply with, even for the same type of data. However, most state laws and the four privacy torts are largely ineffective at filling in the gaps of federal laws.[137] The four privacy torts—intrusion on seclusion, public disclosure of private fact, false light, and misappropriation of image—have been interpreted narrowly, "prevent[ing] their ability to redress data harms" resulting from "contemporary privacy and security problems."[138]

Any business calling the FTC the "de facto data protection authority" would be doing so "at their peril."[139] Instead, companies must be aware of the role state attorneys general serve, as they "also play a critical role . . . investigat[ing] the impacts of security breaches that involve the personal information of their states' residents."[140] At the state level, state attorneys general have played a large role in shaping and enforcing data privacy law. "[E]mbrac[ing] their role as consumer watchdog," state "attorneys general have devoted significant time and energy to privacy and data security enforcement"[141] and have "pioneered baseline privacy norms" through litigation, persuasion, and legislation.[142] State attorneys general "from across the country investigated security breaches at retailers such as Target, Neiman Marcus, Michaels, and Home Depot, as well as at banking institutions such as

133 *See id.*
134 *Id.*
135 *Id.*
136 Solove & Hartzog, *supra* note 19, at 587.
137 *See id.*
138 Danielle Keats Citron, *The Privacy Policymaking of State Attorneys General*, 92 Notre Dame L. Rev. 747, 798 (2016).
139 Divonne Smoyer & Aaron Lancaster, *Think the FTC Is the De Facto U.S. Data Protection Authority? State AGs May Have Something to Say*, IAPP (Dec. 12, 2013), https://iapp.org/news/a/think-the-ftc-is-the-de-facto-u-s-data-protection-authority-state-ags-may/.
140 Burke & Millendorf, *supra* note 3, at 9.
141 Citron, *supra* note 138, at 748, 753.
142 *Id.* at 758–85.

J.P. Morgan Chase."[143] Where there are federal gaps in regulations, state attorneys general "have established privacy norms . . . [and] pressed for thicker consumer privacy protections than those sought by federal agencies."[144] Many states also have unfair and deceptive trade acts and practices ("UDAP") statutes that give state attorneys general the authority "to seek civil penalties, injunctive relief, and attorneys' fees and costs."[145] State UDAP statutes "do not contain the same limitations on recovery of civil penalties as does the FTC Act."[146] Thus, "rather than having one *de facto* [data protection authority] in the FTC, the U.S. actually has 50+ such [data protection authorities]."[147]

To further add to this uneven and fragmented cybersecurity landscape, the European Union's adoption of the GDPR has spurred a number of states to pass new or amended GDPR-inspired data privacy legislation. These new state data breach laws "expand the definition of personal information and specifically mandate that certain information security requirements are implemented."[148] In late June 2018, California signed into law the California Consumer Privacy Act, which will go into effect in January 2020.[149] "California's new privacy law . . . allows consumers to learn what personal information about them is held by businesses, and to opt out of the sale of that information."[150] The wave of new state legislation shows the "increased state interest in closely regulating the means by which personal data is stored and protected—rather than simply imposing requirements and penalties for breach events."[151] Iowa passed a law to take effect on July 1, 2018, which "regulat[es] online services and mobile apps for students" by "prohibit[ing] the use of students' information for certain purposes, such as creating student profiles or selling or renting a student's information."[152] Iowa's law adds to the already-problematic sectoral framework, as it is specific to internet operators who use student information.[153] Additionally, "it requires operators to implement and maintain security procedures and practices appropriate and consistent *with industry standards and applicable state and fed-*

143 Burke & Millendorf, *supra* note 3, at 9.

144 Citron, *supra* note 138, at 785.

145 *Id.* at 750, 754.

146 Smoyer & Lancaster, *supra* note 139.

147 *Id.*

148 Jeewon Kim Serrato et al., *US States Pass Data Protection Laws on the Heels of the GDPR*, NORTON ROSE FULBRIGHT (July 9, 2018), https://www.dataprotectionreport.com/2018/07/u-s-states-pass-data-protection-laws-on-the-heels-of-the-gdpr/.

149 *See* Assemb. B. 375, 2017–18 Leg., Reg. Sess. (Cal. 2018).

150 Wendy Davis, *Advertisers Tell FTC California Privacy Law Threatens Web Economy*, DIGITAL NEWS DAILY (Aug. 22, 2018), https://www.mediapost.com/publications/article/323973/advertisers-tell-ftc-california-privacy-law-threat.html.

151 Sean Ahern, *First Europe, Now the States: Big Changes Coming to State Data Privacy Laws*, JDSUPRA (June 27, 2018), https://www.jdsupra.com/legalnews/first-europe-now-the-states-big-changes-36098/.

152 Serrato et al., *supra* note 148.

153 *Id.*

eral laws, rules, and regulations."[154] But as Part I has demonstrated and as Part II will discuss, compliance consistent with this patchwork of cybersecurity law is unmanageable.

Powerful states may also exert a regulatory effect on other states, aptly labeled the "California effect."[155] Companies are incentivized "to follow the regulatory standards of powerful states" because "stronger state standards are more likely to be adopted . . . and enjoy wide support from policy groups."[156] With California's recent data privacy legislation, companies who deal with the personal data of California residents will be forced "to decide whether to overhaul all their data collecting operations or build in-certain operations solely for their California clients."[157]

While new proposed and enacted state legislation "mirror some of the protections provided by Europe's newly enacted General Data Protection Regulation,"[158] the data privacy acts thus far are significantly narrower than the omnibus of the GDPR. The increasing number of state bills "represents ongoing efforts at the state level to augment and strengthen protections for consumer data privacy—by adding additional requirements on businesses that deal with protected personal data."[159]

II. Challenges to Compliance

Part I discussed how companies face cybersecurity compliance obligations from all directions in the form of a hodgepodge of state, federal, and international statutes; regulatory guidance; and various enforcement actors. The sheer number of obligations companies have within the cybersecurity landscape make it unmanageable and costly for companies to comply. This Part discusses how the current state of cybersecurity compliance is insufficient to achieve the goal of true security of consumers' data.

A. One-Time Check-the-Box Compliance

Many of the companies who have suffered high-profile data breaches over the past few years were actually labeled compliant at the time of the breach.[160] Target was a victim of "what was called an 'epic' security breach," but "was validated as [payment card industry]-compliant just two months

154 *Id.* (emphasis added).

155 Citron, *supra* note 138, at 762 (citing David Vogel, Trading Up 247–70 (1995)).

156 *Id.*

157 Rhys Dipshan, *Corporate Compliance Efforts in the Dark with California Privacy Law*, Legaltech News (July 11, 2018), https://www.law.com/legaltechnews/2018/07/11/corporate-compliance-efforts-in-the-dark-with-california-privacy-law/.

158 Serrato et al., *supra* note 148; *see also* GDPR, *supra* note 112.

159 Ahern, *supra* note 151.

160 Christian Moldes, *Compliant but Not Secure: Why PCI-Certified Companies Are Being Breached*, J. Cyber Security & Info. Sys., May 2018, at 18, 18 ("The number of security breaches in the past two years has increased considerably, even among the companies for which assessors deemed compliant.").

before the breach."[161] In other words, the company was ostensibly complying with the payment card industry data security standard (PCI DSS) when the breach occurred.[162] However, "[o]ne of the major misconceptions about PCI DSS compliance is PCI DSS-certified companies are secure or hacker-proof."[163] Additionally, "only 29 percent of companies are compliant a year after validation," as they often are simply "checking the boxes for PCI DSS compliance off their list . . . and then forgetting about it until the next audit is due."[164] Yet, "compliant" designations were given to Target just "weeks before hackers installed malware on the retailer's network," or for six consecutive years before Heartland Payment Systems suffered a major data breach.[165] Verizon's 2015 PCI compliance report found that not a single company who suffered a breach was fully PCI DSS compliant at the time of the breach.[166] However, meeting compliance standards for the purpose of an audit does not mean that "security controls [are] sustainable or resilient after the initial certification assessment."[167] "Data security programs that employ a 'check-the-box' approach will likely be viewed as ineffective."[168] Many organizations dangerously "assume that . . . compliance is merely passing their annual assessments and obtaining certifications."[169] The problem with this, however, is treating compliance as a "singular event," as opposed to making compliance a "part of the organization's continuous monitoring effort."[170] Security experts even recommend that companies "must build and manage an advanced security program that goes far beyond specific sets of compliance requirements" to keep their data completely protected from criminals.[171]

Additionally, existing "legal rules . . . establish[ ] a floor" and "play[ ] only a limited role in animating corporate processes and practices more broadly."[172] Numerous Chief Privacy Officers ("CPOs") have noted "the limited role that specific legal rules play[ ] in directly shaping their actual under-

161 Kurt Hagerman, *Security vs. Compliance*, ARMOR BLOG (Feb. 16, 2016), https://www.armor.com/blog/security-vs-compliance/.

162 The PCI DSS "is a set of security standards designed to ensure that ALL companies that accept, process, store or transmit credit card information maintain a secure environment." *PCI FAQs*, COMPLIANCEGUIDE.ORG, https://www.pcicomplianceguide.org/faq/#1 (last visited Nov. 28, 2018).

163 Moldes, *supra* note 160, at 20.

164 *Id.*

165 *Id.*

166 *Id.* ("Of all the companies investigated by our forensics team over the last 10 years following a breach, not one was found to have been fully PCI DSS compliant at the time of the breach." (internal quotation marks omitted) (quoting VERIZON, PCI COMPLIANCE REPORT 12 (2015)).

167 *Id.*

168 Davis et al., *supra* note 8, at 650.

169 Moldes, *supra* note 160, at 20.

170 *Id.*

171 Hagerman, *supra* note 161.

172 Kenneth A. Bamberger & Deirdre K. Mulligan, *Privacy on the Books and on the Ground*, 63 STAN. L. REV. 247, 265 (2011).

standing of privacy's meaning," while one CPO in particular pointed out that the statutes merely "enforce the minimum."[173] Thus, it is evident that the compliance standards set forth—in content and in practice—are simply insufficient for companies to achieve actual data security.

B. Unmanageable and Unclear Compliance Demands

Businesses' "[l]itigation concerns are compounded by the piecemeal condition of state and federal laws governing cybersecurity obligations. [This] includes fragmented statutes and regulations, and evolving common law standards that pose an obstacle to formulating stable expectations about cybersecurity behavior."[174] Businesses face "a patchwork of sometimes contradictory state . . . laws" and increasingly aggressive government enforcement.[175] What *is* clear is that the current state of cybersecurity law "does not provide clear guidance to companies that are looking to effectively manage not only cyber incidents themselves, but also attendant liabilities."[176]

While "[t]he specter of fifty state attorneys general pursuing a company for privacy or data security violations is more theoretical than real," a "pile-up effect" concern is still relevant.[177] Companies may face overlapping state and federal actions with duplicative costs. Even if the FTC brings an enforcement action against a company, "[c]ompanies must also watch out for parallel litigation by state attorneys general."[178]

The GDPR has ninety-nine articles spanning 261 pages.[179] For many businesses, especially small businesses, attempting to fully understand the GDPR's requirements on their own may be impossible. Thus, a business may have to hire outside experts to help ensure compliance within its organization. Even though the increasingly stringent data privacy standard of the GDPR is now in effect for all companies that do business with residents of the

173 *Id.* at 266.

174 GERMANO & GOLDMAN, *supra* note 17, at 2.

175 *Id.*

176 *Id.*

177 Citron, *supra* note 138, at 796–97.

178 Kevin LaCroix, *Cybersecurity Enforcement: The FTC Is Out There*, THE D&O DIARY (Apr. 21, 2015), https://www.dandodiary.com/2015/04/articles/cyber-liability/guest-post-cybersecurity-enforcement-the-ftc-is-out-there/ ("Snapchat's case is illustrative. . . . In May 2014, the FTC filed a complaint against Snapchat, alleging that the company made false representations about the disappearance of the snaps, the collection of users' personal data, and the robustness of its data security. Based on these allegations, the FTC asserted that Snapchat had engaged in deceptive practices under section 5 of the FTC Act. In May 2014, Snapchat agreed to settle with the FTC. The consent order prohibited misrepresentations about the company's data privacy and security, required Snapchat to establish a comprehensive privacy program, and imposed independent monitoring and reporting obligations for 20 years. While the FTC enforcement action was pending, the Maryland attorney general advanced similar allegations against Snapchat and claimed violations of Maryland consumer protection law and COPPA. Snapchat agreed to pay $100,000 and take corrective measures in a June 2014 settlement with Maryland."(footnote omitted)).

179 *See supra* note 119 and accompanying text.

European Union, it is still unclear what the exact scope of the laws are. A major criticism of the GDPR is that it "leaves much to interpretation." [180] The GDPR requires companies to take "reasonable steps" and "reasonable measures" but never defines what "reasonable" means.[181] Similarly, with respect to the California Consumer Privacy Act, it is unclear whether the law applies only to consumer personal data, or employee personal data as well.[182] Thus, "most companies will face a hard time complying with the law's data request, consent and deletions mandates."[183] In addition, the Act includes restrictions on financial incentive practices that are "unjust, unreasonable, coercive, or usurious in nature."[184] Exactly what "unjust, unreasonable, coercive, or usurious in nature" means is unclear unless "definitive regulatory guidance" is issued.[185]

As discussed in Section I.B, the compliance expectations provided by the FTC are wholly inadequate. Instead of "issu[ing] any formal regulations or rules related to data security under Section 5 . . . the FTC argues that it 'has been investigating, testifying about, and providing public guidance on companies' data-security obligations under the FTC Act for more than a decade.'"[186] *Wyndham Worldwide* was seen as a "hugely frustrating decision for breach victims," particularly because it validated the FTC's "efforts to punish companies for failing to take 'reasonable' steps to secure sensitive data without giving any guidance about what 'reasonable' is."[187] Critics of the FTC's authority have found it troubling "that the FTC apparently expects businesses to divine from a large number of ad hoc, fact-specific consent decrees with varying provisions what they must do vis-à-vis data security to avoid possible FTC targeting."[188] Companies are expected to rely on "complicated consent decrees for guidance (in the absence of formal agency guidelines or litigated court decisions)," which increases the costs of compliance.[189]

---

180 Michael Nadeau, *General Data Protection Regulation (GDPR): What You Need to Know to Stay Compliant*, CSO (Apr. 23, 2018), https://www.csoonline.com/article/3202771/data-protection/general-data-protection-regulation-gdpr-requirements-deadlines-and-facts.html.

181 *See id.*

182 *See* Dipshan, *supra* note 157.

183 *Id.*

184 *See* Assemb. B. 375, 2017–18 Leg., Reg. Sess. (Cal. 2018).

185 Dipshan, *supra* note 157.

186 Gerard M. Stegmaier & Wendell Bartnick, Essay, *Psychics, Russian Roulette, and Data Security: The FTC's Hidden Data-Security Requirements*, 20 GEO. MASON L. REV. 673, 694 (2013) (quoting Plaintiff's Response in Opposition to Wyndham Hotels and Resorts' Motion to Dismiss at 13, FTC v. Wyndham Worldwide Corp., No. 12-1365, 2013 WL 1222491 (D. Ariz. Mar. 25, 2013) (No. 2:12-cv-01365), 2012 WL 4766957).

187 Grande, *supra* note 47 (internal quotation marks omitted) (quoting Jason Weinstein, partner at Steptoe & Johnson LLP).

188 Abbott, *The Federal Trade Commission*, *supra* note 31, at 5.

189 *Id.*

Even if the FTC finds that a company violated its consent decree, "the process by which it came to that conclusion likely won't be made public."[190] The FTC operates in secrecy, "mak[ing] it difficult to know how its enforcement methods may have failed to prevent [companies] from repeatedly engaging in deceptive privacy practices."[191] This lack of clarity and transparency makes it more difficult for companies to know how to manage their privacy practices moving forward, "highlight[ing] the need for a national privacy law."[192]

III. A Call for Federal Omnibus Regulation and Enforcement

The adoption of the GDPR is itself a huge addition of obligations for companies to the already-messy, piecemeal framework of cybersecurity law. The amount of GDPR-inspired legislation at the state and global levels is only making compliance with cybersecurity law more unmanageable and difficult. Without federal legislation, it will be increasingly tougher for companies to understand how to comply with these regulations; how to best protect themselves from liability; and, most importantly, how to protect consumers' data privacy. Thus, policymakers should consider creating preemptive federal cybersecurity to replace the current fragmented and unworkable approach.

"[P]rospects for federal regulation of cybersecurity and consumer privacy were dim" even during the Obama administration, and "meaningful federal legislation and regulation are nonstarters" within the Trump administration.[193] However, from the hack of Sony, "allegedly orchestrated and sponsored by North Korea,"[194] to the Russian hacking of the 2016 U.S. elections,[195] it is clear that data security has become a "national security issue."[196] Despite the challenges in securing federal regulation of cybersecurity and data privacy, this Note repeats the call for a federal omnibus regulation, a national answer to a national security issue. While there are substantial limits and issues with the FTC's enforcement of data privacy, regulation from a de facto enforcement agency "appears significantly preferable to relying on burgeoning state regulation."[197]

This Note does not argue for a simple copy and paste of the GDPR. Rather, this Note argues for a federal law that carefully considers how to most effectively incentivize true security within businesses.

---

190 Louise Matsakis, *The FTC Is Officially Investigating Facebook's Data Practices*, Wired (Mar. 26, 2018), https://www.wired.com/story/ftc-facebook-data-privacy-investigation/.

191 *Id.*

192 *Id.*

193 Jonathan Mayer, *Data Protection Federalism: Opportunities for State Executive Leadership on Cybersecurity and Consumer Privacy*, Century Found. (Aug. 15, 2018), https://tcf.org/content/report/data-protection-federalism/?agreed=1.

194 Davis et al., *supra* note 8, at 624.

195 *Twelve Russians Charged with US 2016 Election Hack*, BBC (July 13, 2018), https://www.bbc.com/news/world-us-canada-44825345.

196 Davis et al., *supra* note 8, at 624.

197 Abbott, *The Federal Trade Commission*, *supra* note 31, at 9.

A. Benefits of Federalism Do Not Apply in Cybersecurity

Critics may argue that data security and privacy are areas of law that ought to be left to the states. However, the nature of the internet and electronic commerce is not one that is defined by state borders. Electronic commerce and associated data breaches have an "inherently interstate nature."[198] The moment a "developer's app is offered in the iTunes store, consumers in all fifty states can download it,"[199] potentially placing that developer immediately within the scope of every state's cybersecurity and data privacy laws.

One of the biggest benefits of federalism—and one of the biggest criticisms of a federal omnibus privacy law—is that it allows for state experimentation. Critics argue that "[t]he preemptive scope of an omnibus federal privacy law [would be] likely to block new approaches to information privacy."[200] Additionally, states are more often the "first to act in response to new problems or issues, of which many arise in a time of rapid technological and cultural change."[201] While innovation is important, and it is true that innovation and experimentation occur more effectively at the state level, that very experimentation has, in effect, undermined security compliance. Particularly in light of the GDPR, the passage of GDPR-inspired state legislation, and the increasing presence of various state and federal enforcement agencies, it is becoming more difficult for companies to know what to comply with and how to comply effectively. And because of the reality that the "ever-evolving nature of technology creates a moving target for agency enforcement,"[202] it may even be more important that there is a single, centralized enforcement authority, as opposed to fifty dynamic experiments occurring at once, with the expectation that businesses comply.

Additionally, leaving cybersecurity and data privacy laws to the states may allow the most restrictive state policy to dictate.[203] Currently, the FTC is arguably the largest federal enforcement authority in cybersecurity and data privacy. However, its model, as discussed in Section I.B, is highly problematic and limited, despite its growing position as the de facto data protection authority.[204] FTC enforcement initiatives "are supplemented by an increas-

198 *Id.*

199 Citron, *supra* note 138, at 802.

200 Paul M. Schwartz, Essay, *Preemption and Privacy*, 118 YALE L.J. 902, 930 (2009).

201 *Id.*

202 Stegmaier & Bartnick, *supra* note 186, at 695.

203 *See* Citron, *supra* note 138, at 762 ("Companies have a strong incentive to follow the regulatory standards of powerful states. David Vogel has labeled this phenomenon the 'California effect.' . . . In recognition of this phenomenon, Attorney General [Kamala] Harris has said: 'If we can strengthen privacy protections here [in California], we can benefit consumers around the world." (third alteration in original) (footnotes omitted) (quoting Jessica Guynn, *Facebook to Require Privacy Policies for All Apps in App Center*, L.A. TIMES (June 22, 2012), http://articles.latimes.com/2012/jun/22/business/la-fi-facebook-ag-20120622)).

204 *Cf.* Smoyer & Lancaster, *supra* note 139 (noting impact that state attorneys general can have on U.S. data protection).

ing number of state government actions bearing on data security."[205] The cybersecurity landscape, as it stands, is overly difficult to comprehend, which makes it far too costly and unmanageable to comply with. Thus, a centralized and streamlined set of regulations will help further the goal of achieving actual security.

B. Market Failure Requires Increased Federal Involvement

Despite the alarming increase in data breach headlines, "[c]onsumers . . . do not seem to change their buying behavior at those breached merchants,"[206] and "are seemingly less worried about privacy and online security."[207] While a company's "cash flow, cash reserves, [and] capital structure" are affected after a breach, it does not occur "at the hands of consumers."[208] A 2016 study found that "[c]onsumers are quick to return to breached merchants," "return[ing] . . . nearly three months after the breach."[209] The study found that some consumers returned due to a lack of awareness of the breach or were "unfazed . . . in a way that materially change[d] their shopping behavior."[210] Consumer apathy toward data security is growing, to the point where consumers may actually be "simply accepting a certain level of risk when they participate in the digital economy."[211]

While "highly publicized breaches provide one form of incentive," even in high-profile cases like Target, who "paid $39 million to settle a class action lawsuit resulting from the cybersecurity breach of its customers' personal information,"[212] a Deloitte study reported that "56 percent of respondents said they still plan[ned] to shop . . . at retailers that have experienced a data breach."[213] Consumers reported they continue to shop at breached stores for a variety of reasons: the store offers the best prices,[214] they "do not feel

205 Abbott, *The Federal Trade Commission*, *supra* note 31, at 9.

206 Branden R. Williams, Consumer Attitudes Toward Breaches: How Consumers React to Retail Breaches 3 (2016), https://www.brandenwilliams.com/brwpubs/Consumer%20Attitudes%20Toward%20Breaches_FINAL.pdf.

207 Laura Paine, *In the Age of Apathy, Enterprises and Consumers Must Improve Online Security Together*, Security.com (Aug. 23, 2018), https://blog.security.com/security-apathy-enterprises-consumers-must-improve-security/.

208 Williams, *supra* note 206, at 3.

209 *Id.* at 9.

210 *Id.*

211 Paine, *supra* note 207 ("There is a distinct sense and awareness that consumers are losing control of their data, and there is a feeling that little can be done about it.").

212 John J. Chung, *Critical Infrastructure, Cybersecurity, and Market Failure*, 96 Or. L. Rev. 441, 468 (2018).

213 Renee Morad, *Target Makes a Comeback One Year After Security Breach*, Symantec, https://www.lifelock.com/learn-data-breaches-target-makes-comeback-almost-year-security-breach.html (last visited Feb. 6, 2019).

214 *See id.*

enough harm, or simply do not care enough . . . to change their spending behavior."[215]

Even though cybersecurity is regarded as "a matter of national security and defense" and "a public good that benefits all," private entities are relied upon "to provide the public good even though there is little economic incentive to do so."[216] Within the current landscape, companies are not sufficiently incentivized to bolster their cybersecurity defense. Cybersecurity funding by private entities continues to be underfunded, even though "[t]he frequency, complexity, and costs associated with attacks are increasing."[217] Part of the underfunding is because organizations "are unable to accurately quantify the financial value of prospective investments" in cybersecurity defense.[218] The full cost of a cyberattack is not felt by the breached organization, but "borne by numerous unrelated third parties"; thus, "the amount of investment in cybersecurity will not incorporate the full, actual cost of potential harm."[219] If an entity could accurately measure and make the optimal—or even adequate—investment in cybersecurity, the entity "will not be able to charge for the positive externalities it generates."[220]

The costs of achieving true security in compliance with the unevenly layered, changing, and inconsistent patchwork of cybersecurity law are astronomically high. Self-protection does provide an incentive to invest in cybersecurity defenses,[221] and while the immediate cost of handling a security breach may be high, due to consumers' general lack of awareness of breaches, preference for convenience, and apathy toward data security, "[t]he market, by itself, is unable to provide sufficient incentives for an optimal amount of spending on cybersecurity."[222] Thus, the need for a comprehensive preemptive federal cybersecurity law is stronger than ever.

IV. Considerations in Creating Federal Omnibus Legislation

A. Incentivizing Holistic Security

Whether it's the creation of federal legislation or the FTC more definitively promulgating rules, rulemakers should consider what will most effectively lead to true cybersecurity. Federal policymakers may consider adopting a policy that better incentivizes holistic security, as opposed to incentivizing companies to do the bare minimum to escape liability when a breach occurs. Legislation should consider what motivates companies and how companies will navigate such legislation or regulations. One big problem "that surfaces again and again, regardless of [the] regulatory standard[,] . . . [is] failing to

215 Williams, *supra* note 206, at 12.
216 Chung, *supra* note 212, at 457.
217 *Id.* at 470–71.
218 *Id.* at 471.
219 *Id.* at 458.
220 *Id.*
221 *See id.* at 457.
222 *Id.* at 470.

understand the difference between compliance and security."[223] However, "compliance does not equal security—it's merely a snapshot of how your security program meets a specific set of security requirements at a given moment in time."[224] Organizations often conflate the two and "get so consumed by complicated regulations that they stop focusing on security altogether."[225] However, when companies are faced with the threat of liability accompanied by heavy sanctions, they focus on the complicated regulations instead of focusing on what security measures make sense. This is worsened when the regulations are not sufficient to achieve actual security.

One way to consider better incentivizing security is by offering companies an affirmative defense to a certain level of liability after a breach occurs. Ohio recently signed into law the Data Protection Act, "which provides businesses with an affirmative defense to data breach claims if the business was in compliance with reasonable security measures at the time of the breach."[226] Thus, Ohio offers a safe harbor defense, providing an innovative way to incentivize cybersecurity compliance. Instead of seeking to "motivate through threat of punitive measures, Ohio's [Data Protection Act] offers a fresh and affirmative step forward"[227] and seeks "to be an incentive and to encourage businesses to achieve a higher level of cybersecurity through voluntary action."[228] The Act "will be the first in the nation [that] incentivizes businesses to implement certain cybersecurity controls by providing them with an affirmative defense."[229] Affirmative defenses, however, may just incentivize companies to do the bare minimum to successfully assert the affirmative defense to escape liability.[230] Thus, offering a safe harbor or

223 Hagerman, *supra* note 161 ("The most common misconception? Thinking compliance and security are one and same.").

224 *Id.*

225 *Id.*

226 Dena Castricone, *Compliance with Established Cybersecurity Standards Provides Protection from Liability in Ohio*, JDSUPRA (Aug. 9, 2018), https://www.jdsupra.com/legalnews/compliance-with-established-15509/.

227 Jeffrey T. Cox, *New Ohio Data Protection Law Incentivizes Business Community to Institutionalize Cybersecurity*, LEXOLOGY (Aug. 13, 2018), https://www.lexology.com/library/detail.aspx?g=7b0bb9fa-ed91-4fd6-b56e-65909690d362.

228 John Landolfi & Chris Ingram, *New Ohio Law Incentivizes Businesses that Comply with Cybersecurity Programs*, COLUMBUS BUS. FIRST (Sept. 20, 2018) (internal quotation marks omitted) (quoting S.B. 220, 132 Gen. Assemb. (Ohio 2018), https://www.bizjournals.com/columbus/news/2018/09/20/new-ohio-law-incentivizes-businesses-that-comply.html).

229 *Id.*

230 For example, the *Faragher-Ellerth* affirmative defense available to employers in Title VII sexual harassment lawsuits is easily satisfied if an employer can show that (1) it took reasonable steps to prevent and correct sexual harassment in the workplace, and (2) the employee failed to take advantage of the employer's preventive or corrective measures. *See* Joseph A. Seiner, *Plausibility Beyond the Complaint*, 53 WM. & MARY L. REV. 987, 1018–21 (2012). Thus, employers have been incentivized to create antiharassment policies and make reasonable efforts to disseminate those policies. However, in the wake of the #MeToo movement, those "reasonable" efforts, while protecting employers from liability, evidently did little to effect change in workplace culture. *See* Lauren Stiller Rikleen,

affirmative defense to businesses may be effective for incentivizing cybersecurity compliance, but should be structured in a way that sets the bar high, such that the minimum baseline offers some effective level of data security. Various affirmative defenses could be used in conditioning disclosure requirements on a business's level of security, similar to how the GDPR fashions its disclosure requirements.

Some have questioned whether "imposing massive liability on a company that falls victim to a data breach [is] truly the best way to protect consumer data."[231] This criticism is called even more into question when companies are required to fully understand and comply with a "patchwork quilt of state data breach laws [which] presents a compliance quagmire for businesses."[232] Companies may want to avoid fines, but if the fines are too small they may be regarded as a cost of doing business. Additionally, if the ceiling for fines is too high and the actual threat of fines too uncertain, the threat of sanctioning high penalties may not be very effective.[233] For the Cambridge Analytica breach, Facebook's penalty—$40,000 per violation multiplied by over eighty-seven million users affected—"could theoretically add up to trillions of dollars."[234] Despite this, there is doubt that the FTC would ever fine such an amount.[235] For sanctions to be effective, "a certainty threshold . . . has to be met," which "requires successful prosecution and sanctioning."[236] However, oftentimes "enforcement authorities fail to collect the fines they issue[ ]," which further reduces the efficacy of sanction threats.[237]

B. Leverage Reputational Harm

While reputational harm currently has limited import,[238] it could be better leveraged to play a role in incentivizing companies to implement measures that help protect against hackers and data breaches. In addition to the costs of data privacy litigation and potential penalties, companies' reputations still suffer, causing them to lose out on potential revenue. Fifty-four percent of over 7000 public companies "had an incident in the past two and half years that materially impacted their reputation," which led to "a loss of

Faragher-Ellerth *at 20: How Far Have We Come? And Where Do We Need to Go?*, A.B.A.: LAB. & EMP. L., Spring 2018, at 1, 1.

231 Grossman, *supra* note 9, at 1283.

232 Cox, *supra* note 227.

233 *See* Benjamin van Rooij & Adam Fine, *How to Punish a Corporation: Insights from Social and Behavioral Science*, COMPLIANCE & ENFORCEMENT (Sept. 1, 2017), https://wp.nyu.edu/compliance_enforcement/2017/09/01/how-to-punish-a-corporation-insights-from-social-and-behavioral-science/.

234 Cao, *supra* note 18.

235 *Id.*

236 Rooij & Fine, *supra* note 233.

237 *Id.* ("Fine collection rates have been well below 50% across different enforcement agencies, with the DOJ only collecting 4% of penalties imposed.").

238 *See supra* Section III.B.

trust."[239] According to a KPMG study, nineteen percent of consumers completely stopped shopping at a retailer after a breach, and thirty-three percent took a break from shopping at that retailer for an extended period.[240] While another study found that "[o]nly 4% [of consumers] took their business to a competitor that they perceived to be more secure, with an additional 2% indicating they did not return specifically because of the breach," it is at least clear that companies suffer from "the digital equivalent of a natural disaster . . . [which] causes a minor interruption in operations with a significant capital outlay to clean up and return to normal operations."[241]

However, the risk of reputational harm may not affect all companies equally. Reputational costs are higher for "companies in industries such as banking, utilities, and travel and transportation," and trust may play a bigger role when "consumers tie their values to products they purchase and the companies they work for."[242] The reputation incentive may be limited by how much press is devoted to a company's data breach, and the amount of press devoted to a particular data breach may be determined by how large a company is, how badly the company got it wrong, or how many total users were affected. When "the general public rarely pays attention to FTC privacy actions," the reputational harm may only occur if the privacy action is amplified on social media or on the news.[243] Within the privacy sphere, reputational damage may be more limited as it is "largely within the community of privacy professionals and the entities that do business with a particular company."[244]

One way to better leverage reputational harm incentives may be to implement a National Cybersecurity Index, similar to Transparency International's Corruption Perceptions Index.[245] On the Corruption Perceptions Index, countries are scored on a "scale of 0 (highly corrupt) to 100 (very clean)."[246] In addition to each country's score in rank order, the Corruption Perceptions Index includes the previous four years for comparison. In the cybersecurity context, companies could be rated on a scale of zero (highly susceptible to data breaches) to 100 (highly secure). Just as "[n]o country gets close to a perfect score in the Corruption Perceptions Index," it may be likely that there is no company that gets close to a perfect security score.[247] However, companies may be motivated by an external score to be the most

239 Mengqi Sun, *What Loss of Trust Costs Companies in Dollars and Cents*, WALL ST. J. (Oct. 31, 2018), https://blogs.wsj.com/riskandcompliance/2018/10/31/what-loss-of-trust-costs-companies-in-dollars-and-cents/?mod=relatedInsights.

240 Green & Hanbury, *supra* note 5.

241 WILLIAMS, *supra* note 206, at 11–12.

242 Sun, *supra* note 239.

243 Solove & Hartzog, *supra* note 19, at 606.

244 *Id.*

245 *Corruption Perceptions Index 2016*, TRANSPARENCY INT'L (Jan. 25, 2017), https://www.transparency.org/news/feature/corruption_perceptions_index_2016?gclid=eaIaIQobChMI4qzwt-763gIVUbbACh2Q4gwKEAAYASABEgKLz_D_BwE#table.

246 *Id.*

247 *Id.*

highly secure company within its industry or to improve its score year after year. Additionally, a Cybersecurity Index could serve as a central database for all data breaches, so consumers can confirm the security history of a company before deciding to start or continue using a company's product or service. Additionally, a centralized database may help combat consumers' general lack of awareness of data breaches.[248]

Of course, the risk of creating a Cybersecurity Index or ratings system is that if a highly rated company experiences a breach, trust diminishes in the Index, and it may lose its value. Countries at the bottom of the Corruption Perceptions Index, because of their endemic corruption, may not care that they fall at the bottom of the Index, but a low Cybersecurity Index score is essentially a broadly advertised statement of distrust, and as discussed above, loss of trust can have a substantial impact on a company's "profitability, growth and sustainability."[249]

C. Consider a Different Standard for Small Businesses

Policymakers should also consider the impact of compliance regulations and standards on small businesses. The costs of compliance, as well as the cost of a data breach, are significantly worse for small businesses. All of these complex compliance issues are magnified for small businesses, who may not have the personnel or resources to understand regulations, implement programs, or ensure security. At the same time, "[t]he National Cyber Security Alliance claims that one in five small businesses gets hacked every year," reflecting the increased risk posed for small businesses.[250] Many smaller businesses may be "tempt[ed] to ignore [security vulnerabilities] because of a lack of personnel or sizable resources to dedicate to cybersecurity. However, this is precisely what makes these businesses a prime target."[251] And once a small business gets hacked, "sixty percent go bankrupt within six months."[252] "[T]he average cost of a single data breach [for small- and medium-sized enterprises] can be as much as $117,000." [253] An alternative standard, however, should not be based solely on the size of the company, but perhaps on the type of information collected or the amount of data collected. A small company handling the most sensitive privacy information should not be subjected to a laxer standard simply because it is a smaller company. However, even a heightened security standard for smaller companies that is streamlined may make it more feasible for smaller companies to comply.

---

248 *See supra* Section III.B.

249 Sun, *supra* note 239.

250 Noah G. Susskind, Note, *Cybersecurity Compliance and Risk Management Strategies: What Directors, Officers, and Managers Need to Know*, 11 N.Y.U. J.L. & BUS. 573, 578–79 (2015) ("[S]mall businesses often fail to realize what lucrative targets they are.").

251 T.J. DeGroat, *Security Audits and Penetration Testing*, SPRINGBOARD BLOG (July 10, 2018), https://www.springboard.com/blog/security-audits-and-penetration-testing/.

252 Susskind, *supra* note 250, at 578.

253 DeGroat, *supra* note 251.

D. Increase Regularity of Security Audits and Penetration Tests

As discussed in Section II.A, companies that are deemed compliant have suffered high-profile data breaches over the past several years. These organizations tend to only appear compliant on the day of the security audit, and it is only the snapshot of the company's compliance program at that particular moment in time that looks secure. Organizations would benefit from greater visibility and control of all data locations, greater security awareness by all of the organization's stakeholders, and regular self-assessments.[254] Ensuring continuous monitoring could be achieved through establishing a federal agency or an independent agency[255] that would regularly and randomly perform security audits and penetration tests. A security audit is "a systematic evaluation of . . . enterprise IT infrastructure defenses," which can evaluate a company's past and future risks.[256] Data breach response plans are often ineffective because they are not reviewed often enough or in a timely manner.[257] In a 2014 study, thirty-seven percent of companies "[had] not reviewed or updated [its data breach response plan] since it was put in place."[258] Forty-one percent of companies had "[n]o set time period for reviewing and updating the plan."[259] Fourteen percent reviewed and updated their plans "[o]nce each year," five percent reviewed and updated their plans "[t]wice per year," and only three percent reviewed and updated their plans "[e]ach quarter."[260] However, security audits are insufficient alone, as they are merely snapshots at a given point in time. Penetration tests, however, "go beyond security audits . . . by trying to breach [a company's] system just like a hacker. In this scenario, a security expert will try to replicate the same methods employed by bad actors to determine if [a company's] IT infrastructure could withstand a similar attack."[261]

V. CRITIQUES

Solove and Hartzog are proponents of the FTC's privacy jurisprudence serving as a functional equivalent body of common law.[262] They argue that through the FTC's settlement agreements with companies, the FTC has actually created a "robust privacy regulatory regime,"[263] and that despite criticism of the FTC, "the FTC has *not* been arbitrary and unpredictable in its enforce-

254 *See* GERMANO & GOLDMAN, *supra* note 17, at 6; Moldes, *supra* note 160, at 20.

255 An independent security auditing agency could be set up similar to how independent accounting firms serve public companies.

256 DeGroat, *supra* note 251.

257 PONEMON INST., IS YOUR COMPANY READY FOR A BIG DATA BREACH? 5 (2014), https://www.ponemon.org/blog/is-your-company-ready-for-a-big-data-breach-the-second-annual-study-on-data-breach-preparedness.

258 *Id.*

259 *Id.* fig.3.

260 *Id.*

261 DeGroat, *supra* note 251.

262 Solove & Hartzog, *supra* note 19, at 586.

263 *Id.*

ment."[264] However, their argument that the FTC's settlement agreements have created a body of common law "does not adequately address the questions of whether the FTC is appropriately applying its Section 5 authority in finding unfairness and deception and whether it is imposing undue burdens on business by failing to provide any guidance beyond that found in fact-bound case-specific decrees."[265]

Additionally, the expectation that companies should look to the FTC's settlement agreements as a body of law to adhere to is problematic, as a major motivator to settling and agreeing to a consent order is to avoid the costs of going to trial.[266] Even Solove and Hartzog concede that a reason that many of these cases hardly ever make it to court "might be that it is too costly."[267] As there is "no threat of financial penalties for violating Section 5 . . . there is little financial incentive to spend a great deal of time and resources fighting FTC complaints."[268] A recent example is "LabMD, . . . [which] went out of business in the course of litigating against the commission."[269] Additionally, companies may be "reluctant to challenge administration complaints . . . [because] in administrative adjudication, a 'reviewing court must also accord substantial deference to Commission interpretation of the FTC Act and other applicable federal laws,'"[270] which would "make[ ] a challenger's victory less likely and risks the creation of an adverse precedent."[271] Additionally, even if it were conceded that the FTC's "common law jurisprudence" was clear and developed, there still remains a massive patchwork of state and federal laws that companies must comply with. And with the GDPR in effect, many companies must also figure out how to comply with international law.

There is also concern that "[d]ata-security enforcement standards cannot be so rigid as to stifle business growth or give hackers time to exploit the rules."[272] By increasing federal regulation, we run "the risk that federal overregulation will undermine innovation, harm businesses, and weaken the

264 *Id.* at 608.

265 Abbott, *The Federal Trade Commission*, *supra* note 31, at 4 n.19.

266 *See* Solove & Hartzog, *supra* note 19, at 611–13 ("Settling with the FTC . . . allows for companies to 'eliminate the uncertainty and expense of lengthy negotiation and pretrial preparation and litigation.'" (quoting 1 STEPHANIE W. KANWIT, FEDERAL TRADE COMMISSION § 12:4 (2013))).

267 *Id.* at 611.

268 *Id.*

269 Frankel, *supra* note 106.

270 Solove & Hartzog, *supra* note 19, at 613 (quoting *A Brief Overview of the Federal Trade Commission's Investigative and Law Enforcement Authority*, FED. TRADE COMMISSION, https://www.ftc.gov/about-ftc/what-we-do/enforcement-authority (last revised July 2008)).

271 *Id.*

272 Gordon, *supra* note 15, at 204 (internal quotation marks omitted) (quoting Amanda R. Moncada, Comment, *When a Data Breach Comes A-Knockin', the FTC Comes A-Blockin': Extending the FTC's Authority to Cover Data-Security Breaches*, 64 DEPAUL L. REV. 911, 941 (2015)).

economy."[273] However, these concerns must be weighed against what is currently happening: companies are unable to sift through the patchwork of cybersecurity regulations and struggle to comply, making them likelier targets for hackers. For small companies, the risk of maintaining noncompliant practices means being subject to significant financial liability from a wide range of government actors. The risk of getting breached means potentially going bankrupt.

Conclusion

The current state of cybersecurity law is unclear and unmanageable, and given the increasing frequency of high-profile data breaches, it remains an urgent priority to national security. This Note makes a call for an omnibus federal privacy law that would carry a preemptive effect over of state cybersecurity and data privacy laws. The benefits of federalism are outweighed by the increasingly evident costs for companies attempting to secure themselves from not just hackers, but also liability. Data security has become a national security issue urgently requiring a national solution. This omnibus federal privacy law should consider avoiding minimum baseline standards and incentivize businesses to adopt holistic and continuous security.

273 Alden Abbott, Wyndham *Decision Highlights FTC Role in Cybersecurity: Legal and Policy Considerations*, Truth on Mkt. (Sept. 1, 2015), https://truthonthemarket.com/2015/09/01/wyndham-decision-highlights-ftc-role-in-cybersecurity-legal-and-policy-considerations/.