2019

The Duty of Data Security

William McGeveran
University of Minnesota Law School, billmcg@umn.edu

Article

The Duty of Data Security

William McGeveran†

† Associate Dean for Academic Affairs, Professor of Law, and Solly Robins Distinguished Research Fellow, University of Minnesota Law School. I benefited from presenting drafts of this work in progress at the Privacy Law Scholars Conference hosted by the University of California at Berkeley; the Northeast Privacy Law Scholars Workshop hosted by New York Law School and Fordham Law School; and conferences or workshops sponsored by Notre Dame Law School, the University of North Carolina School of Law, and the University of Minnesota Law School. Many thanks for especially valuable comments from Danielle Citron, Julie Cohen, Gautam Hans, Ryan Harkins, Woody Hartzog, Chris Hoofnagle, Gus Hurwitz, Mike Johnson, Margot Kaminski, Anne Klinefelter, Jeff Kosseff, Andrea Matwyshyn, Mark McKenna, Ed McNicholas, Joel Reidenberg, Sharon Sandeen, Peter Swire, David Thaw, and many colleagues on my own faculty. I am indebted to my excellent student research assistants, Richard Canada and Hannah Nelson, and to the staff of the University of Minnesota Law Library, particularly Scott Dewey and Connie Lenz.

INTRODUCTION

When Equifax, the credit reporting agency and data broker, revealed that it had suffered a massive breach compromising personal information of 143 million people, the public reaction was understandable outrage.[1] Subsequent news about Equifax's apparent lapse in competence—failure to install a simple software patch that had been available for two months—quite justifiably increased that anger.[2] The question naturally arose: what precautions does the law require of firms like Equifax, who hold personal data about ordinary Americans that can be highly vulnerable to hacking, theft, leaking, or other misuse? What was Equifax's duty of data security?

Some observers suggest that there is no valid answer to such questions. According to them, the law is insufficiently specific, concrete, or uniform, creating "uncertainty among businesses regarding the appropriate standards for data security."[3] Lawyers fighting against Federal Trade Commission (FTC) enforcement actions in data security cases have been particularly vociferous, arguing that there is no way to understand the meaning of "reasonable" data security measures under consumer protection law.

1. *See* Brian Krebs, *Breach at Equifax May Impact 143M Americans*, KREBS ON SECURITY (Sept. 17, 2017), https://krebsonsecurity.com/2017/09/breach-at-equifax-may-impact-143m-americans; Lauren Zumbach, *Massive Equifax Data Breach Prompts Outrage, Investigations, Bills to Ban Credit Freeze Fees*, CHI. TRIB. (Sept. 16, 2017), http://www.chicagotribune.com/business/ct-equifax-data-breach-0917-biz-20170915-story.html.

2. *See, e.g.*, Lily Hay Newman, *Equifax Officially Has No Excuse*, WIRED (Sept. 14, 2017), https://www.wired.com/story/equifax-breach-no-excuse.

3. Robert L. Rabin, *Perspectives on Privacy, Data Security, and Tort Law*, 66 DEPAUL L. REV. 313, 324 (2017); *see also* Jay P. Kesan & Carol M. Hayes, *Strengthening Cybersecurity with Cyber Insurance Markets and Better Risk Assessment*, 102 MINN. L. REV. 191, 207 (2017) (expressing concern that cybersecurity law is merely "a patchwork of fixes scattered throughout different levels of government" and calling for more "concrete guidance"); Jeff Kosseff, *Positive Cybersecurity Law: Creating a Consistent and Incentive-Based System*, 19 CHAP. L. REV. 401, 410–11 (2016) (suggesting that a federal regulator should provide "binding, concrete guidance" about a host of specific decisions from the strength of encryption to the length of passwords).

One defendant claimed the FTC could "hold virtually any business in the land liable for violating an unknown (and unknowable) standard."[4] The Chamber of Commerce submitted an amicus curiae brief in another case protesting that the law "gives *no* advance notice to businesses of what they should do in a rapidly changing technological environment."[5] A major 2018 decision by the Eleventh Circuit in *LabMD, Inc. v. FTC* partially accepted such contentions.[6]

These claims are balderdash. In fact, the numerous sources of a duty of data security sound together in harmony, not cacophony. Both public law and the private sector have converged on a clear understanding of the duty of data security owed by companies like Equifax when they store personal data. Regulated parties are already shaping their data security measures in response. Like most businesses, they try to do so with common sense: they weigh costs and benefits, assess risk, and invest accordingly.[7] For their part, federal and state regulators (including but not limited to the FTC) have endorsed this set of foundational expectations for reasonable and appropriate security precautions.[8] Experts involved in the daily labor of data security certainly recognize these contours of responsible data security, and may even regard them as somewhat obvious.[9] This is the

4. Appellant's Opening Brief & Joint Appendix Vol. 1, pp. JA1–55 at 36, FTC v. Wyndham Worldwide Corp., 799 F.3d 236 (3d Cir. 2014) (No. 14-3514), 2014 WL 5106183, at *36 (citations omitted); *see also* Timothy E. Deal, Note, *Moving Beyond "Reasonable": Clarifying the FTC's Use of Its Unfairness Authority in Data Security Enforcement Actions*, 84 FORDHAM L. REV. 2227, 2243 (2016) (presenting "overarching concerns that the FTC has not provided companies with sufficient guidance as to what it considers to be 'reasonable' data security practices").

5. Brief for Chamber of Commerce of the United States of America as Amicus Curiae Supporting Petitioner at 11, LabMD, Inc. v. FTC, No. 16-16270 (11th Cir. Jan. 3, 2017). The author of this Article signed an amicus curiae brief taking the opposite position in the same case.

6. 894 F.3d 1221, 1237 (11th Cir. 2018) (vacating the FTC's order requiring "reasonable" data security practices because it "says precious little about how this is to be accomplished"). *But see* FTC v. Wyndham Worldwide Corp., 799 F.3d 236, 255–59 (3d Cir. 2014) (stating that the court has "little trouble rejecting" the claim that a company lacked fair notice of the requirements necessary to fulfill its duty of data security).

7. *See* KENNETH A. BAMBERGER & DEIRDRE K. MULLIGAN, PRIVACY ON THE GROUND: DRIVING CORPORATE BEHAVIOR IN THE UNITED STATES AND EUROPE 27–33 (2015).

8. *See* William McGeveran, *Friending the Privacy Regulators*, 58 ARIZ. L. REV. 959 (2016).

9. *See infra* Part I.B.3.

modern duty of data security. It is every bit as clear as many other legal duties concerning complex topics.

Of course, there are serious issues concerning the *enforcement* of data security law. The *LabMD* decision brings to a head a simmering debate about the appropriate scope of the FTC's authority over data security.[10] The law still struggles with the measurement of harm and damages from security failures.[11] Companies systematically underinvest in security, many regulators lack adequate resources to effectively oversee giant corporations' deployment of fast-moving technologies, and there may be a need for more vigorous ongoing monitoring of compliance rather than a reliance on investigations triggered by security failures.[12] Some scholars have even proposed a strict liability standard for data breaches.[13] This Article stands apart from all these important issues, because it focuses on the *content* of the duty of data security, not the means by which it might be enforced.

10. *See, e.g.*, Woodrow Hartzog & Daniel J. Solove, *The Scope and Potential of FTC Data Protection*, 83 GEO. WASH. L. REV. 2230 (2015) (arguing the FTC's jurisdiction to regulate data protection extends beyond the authority it has already exercised); Justin (Gus) Hurwitz, *Data Security and the FTC's UnCommon Law*, 101 IOWA L. REV. 955 (2016) (arguing the FTC's "common-law" approach to regulating data protection creates unsound law and raises jurisdictional and due process concerns); Michael D. Scott, *The FTC, the Unfairness Doctrine, and Data Security Breach Litigation: Has the Commission Gone Too Far?*, 60 ADMIN. L. REV. 127 (2008) (exploring whether the FTC's actions have exceeded its authority and proposing legislation that that would give the FTC authority to take action "only under well-defined guidelines").

11. *See, e.g.*, George Ashenmacher, *Indignity: Redefining the Harm Caused by Data Breaches*, 51 WAKE FOREST L. REV. 1 (2016) (discussing what harm individuals suffer in the wake of a data breach when they are not yet victims of identity theft, and looking at whether the law responds to harms that do not occur); Rabin, *supra* note 3 (exploring tort remedies available in the wake of a data breach); Daniel J. Solove & Danielle Keats Citron, *Risk and Anxiety: A Theory of Data-Breach Harms*, 96 TEX. L. REV. 737 (2018) (discussing why courts have struggled to conceptualize the harm that occurs after a data breach).

12. *See generally* Eldar Haber & Tal Zarsky, *Cybersecurity for Infrastructure: A Critical Analysis*, 44 FLA. ST. U. L. REV. 515 (2017) (discussing some of the problems with current critical infrastructure protection models and proposing a new model that helps address these problems).

13. *See* Danielle Keats Citron, *Reservoirs of Danger: The Evolution of Public and Private Law at the Dawn of the Information Age*, 80 S. CAL. L. REV. 241, 277–96 (2007) (arguing courts should adopt a strict liability standard with regard to data breaches).

Instead, this Article defines the duty of data security. It examines fourteen different "frameworks" that impose data security obligations on private companies. It demonstrates how these frameworks are clearly converging on a common set of standards for data security in the United States.[14] And finally, it explains why that outcome is both highly familiar in the law and also desirable, notwithstanding objections that law should present cookbook-recipe rules instead of reasonableness-based standards.

Part I of this Article reviews fourteen data security frameworks; seven of them were promulgated by formal legal institutions such as legislatures or regulatory agencies, and seven were derived from private ordering with little or no government involvement. Part II then synthesizes the shared features of the fourteen frameworks, distilling them to describe the features of the duty of data security consistent across different frameworks—and thus across different laws, industry practices, and enforcement mechanisms.

Part III turns to normative matters. It demonstrates how this bottom-up approach of absorbing standards from industry has always been commonplace in the law. From the *lex mercatoria* of medieval times to Judge Hand's formula of $B > PL$ to modern administrative law's theories of new governance, law has always developed in the way the duty of data security is now developing. Moreover, the resulting consensus about the duty of data security is a wise one—principles-based, adjustable to the size and risk profile of the data custodian, nimble enough to incorporate new technological developments, and deferential to the expertise of a growing profession.

A duty of data security grounded in reasonableness principles leaves a great deal of discretion to regulated parties themselves. This need not mean it is toothless, however.[15] The law can set demanding standards and leave individual institutions to determine how to comply in their particular circumstances. The approach I describe here is also consistent with an increasingly influential school of thought that suggests we should view

14. I do not attempt to analyze the distinct structure of data security law in countries outside the United States. *See, e.g.*, Rita Heimes, *Top 10 Operational Impacts of the GDPR: Part 1 - Data Security and Breach Notification*, IAPP PRIVACY ADVISOR (Jan. 6, 2016), https://iapp.org/news/a/top-10 -operational-impacts-of-the-gdpr-part-1-data-security-and-breach-notification (discussing new European Union data security requirements).

15. *See* McGeveran, *supra* note 8.

the requirements of privacy through the prism of "trust," and treat the entities that handle personal information as something akin to "information fiduciaries."[16] For this reason, throughout the Article I refer to organizations handling personal information as *data custodians*. Even though these requirements do not share all the attributes of fiduciary duties, the security frameworks discussed in this Article do impose a special duty on these data custodians. They must dedicate systematic effort toward the safekeeping of the personal information they hold.

Arguing that the duty of data security is clear does not suggest it is easy. Airplanes come with instruction manuals, but that does not mean that just anybody can fly them; thankfully, pilots receive extensive training. Developing a data security program requires considerable judgment and expertise in both management and information technology (IT), which is part of the reason so many responsible data custodians hire specialized chief information security officers (CISOs) and similar leaders.[17] Professionals with security-related certifications are among the highest paid people in IT because their skills are so valuable.[18] Data custodians must rely on them for the complex work of achieving reasonable and appropriate data security.

So then, enforcement challenges remain, the law must ensure that data custodians take their role seriously, and data security is a complex problem that requires expertise. All of this is true, but none of it obscures the central claim of this Article: we already know what the duty of data security is. Existing legal materials and private sector guidance about best practices pro-

16. *See, e.g.*, ARI EZRA WALDMAN, PRIVACY AS TRUST: INFORMATION PRIVACY FOR AN INFORMATION AGE (2018); Jack M. Balkin, *Information Fiduciaries and the First Amendment*, 49 U. CAL. DAVIS L. REV. 1183 (2016); Neil Richards & Woodrow Hartzog, *Privacy's Trust Gap*, 126 YALE L. J. 1180 (2017); Neil Richards & Woodrow Hartzog, *Taking Trust Seriously in Privacy Law*, 19 STAN. TECH. L. REV. 431 (2016); Tim Wu, Opinion, *An American Alternative to Europe's Privacy Law*, N.Y. TIMES (May 30, 2018), https://www.nytimes.com/2018/05/30/opinion/europe-america-privacy-gdpr.html.

17. *See* Aileen Alexander & Jamey Cummings, *The Rise of the Chief Information Security Officer*, KORN FERRY INST. PEOPLE & STRATEGY J., Winter 2016, at 10–11 (reporting that executive consulting firm KornFerry "has seen an explosion in the number of companies across a spectrum of industries that are beefing up their information security teams," including hiring CISOs and giving them more responsibility).

18. *See* GLOB. KNOWLEDGE, 2017 IT SKILLS AND SALARY REPORT 26–30 (2017), https://images.globalknowledge.com/wwwimages/web/salary-report/past-reports/2017-it-skills-salary-report-global-knowledge-en-ww.pdf.

vide data custodians with ample notice about legal responsibilities. And the current degree of clarity is adequate, typical of other legal regimes, and normatively desirable. Let us turn now to fourteen different sources of that duty, and see how all of them say much the same thing.

I. SOURCES OF THE DUTY OF DATA SECURITY

Before describing the duty of data security, we first need to differentiate "data security" from some other concepts with which it is often conflated. *Data security* is just one element of the broader concept of *data privacy*; the latter also relates to the collection, use, and disclosure or personal data in addition to its secure storage. Data security is not quite the same thing as *cybersecurity* either. Data security protects the personal information held by an entity; cybersecurity protects the network's infrastructure.[19] The latter is best understood to include the integrity of the network itself and the prevention of problems like distributed denial of service (DDoS) attacks[20] or deployment of ransomware such as the WannaCry bug.[21] These concepts may overlap in particular cases, such as the use of a zero-day exploit to steal personal data. They remain entirely distinct in other scenarios, such as a hacker deleting company documents that contain no personal data (cybersecurity only) or the theft of paper files containing personal information (data security only).[22] In this Article, "data security" is the protection of personal data,

19. For sources grappling with the definitional boundaries between and among these terms, see, for example, FIN. INDUS. REGULATORY AUTH., REPORT ON CYBERSECURITY PRACTICES (2015) [hereinafter FINRA REPORT], http://www.finra.org/sites/default/files/p602363%20Report%20on%20Cybersecurity%20Practices_0.pdf; SCOTT J. SHACKELFORD, MANAGING CYBER ATTACKS IN INTERNATIONAL LAW, BUSINESS, AND RELATIONS: IN SEARCH OF CYBER PEACE 5–15 (2014); Kosseff, *supra* note 3, at 404–05 (2016); Kirk J. Nahra, *Mastering Cybersecurity by Learning Data Security*, 12 PRIVACY & SECURITY L. REP. 1525 (2013).

20. These typically are attacks that use botnets to overwhelm servers with traffic until they cannot function. *See* Kim Zetter, *Hacker Lexicon: What Are DoS and DDoS Attacks?*, WIRED (Jan. 16, 2016), https://www.wired.com/2016/01/hacker-lexicon-what-are-dos-and-ddos-attacks.

21. *See* Ian Sherr, *WannaCry Ransomware: Everything You Need to Know*, CNET (May 19, 2017), https://www.cnet.com/news/wannacry-wannacrypt-uiwix-ransomware-everything-you-need-to-know.

22. *Cf.* Edward R. McNicholas & Vivek K. Mohan, *An Introduction to the Law of Cyber Risk*, *in* CYBERSECURITY: A PRACTICAL GUIDE TO THE LAW OF CYBER RISK 1-1, at 1-1 to 1-14 (Edward R. McNicholas & Vivek K. Mohan eds., 2016) [hereinafter CYBERSECURITY: A PRACTICAL GUIDE] (distinguishing concepts of privacy, cybersecurity, and surveillance).

digital or otherwise, against access that is not authorized by the data custodian.[23]

The prevalent sense that legal duties under data security law are complicated and disorganized originates in part from the many disparate sources of relevant obligations. We shall see later in the Article that these sources cohere around similar concepts. But first, this Part maps the sources of the duty of data security, and identifies fourteen specific frameworks that exemplify the field. By a "framework," I simply mean a particular set of requirements that impose a duty of data security on custodians of personal data.[24]

I have chosen frameworks that are typical and that, taken together, represent the breadth of different sources of data security obligations. Importantly, I could have chosen other examples. For instance, while the CISSP is perhaps the most widely known, there are numerous competing and complementary certifications for data security professionals.[25] The key point is that these other certifications resemble the CISSP in the fundamental features described later in the Article.[26]

The fourteen frameworks discussed in this Article include seven that come directly from traditional legal sources such as statutes or government agency regulations, and seven that emerge from private ordering within industry rather than from formal law. I discuss the former in Section A and the latter in Section B. These are further divided, for ease of explanation, into a few topical categories. The following chart summarizes the fourteen frameworks examined in the remainder of Part I:

23. Data privacy may also encompass *intentional* collection or use of data by the custodian against the interests of the data subject, but those issues are distinct from the data security concerns that arise from unauthorized access or use.

24. I want to avoid the language of "law," because half of the frameworks are not formal legal requirements. *See infra* Part I.B. I also do not want to describe them as "rules" because, as we shall see, they are usually standards rather than rules. *See infra* Part III.A.

25. *See CISSP – The World's Premier Cybersecurity Certification*, (ISC)², https://www.isc2.org/Certifications/CISSP# (last visited Nov. 20, 2018); *infra* Part I.B.3 (describing the landscape of security-oriented certifications).

26. *See infra* Part II.

LEGAL	**Federal Sectoral Regulation**	HIPAA Security Rule
		Safeguards Rule
	Consumer Protection Regulation	FTC Section 5 Enforcement and State UDAP Enforcement
	State Notification Laws	Breach Notification Statutes
	State Security-Specific Regulation	Massachusetts and New York
		California
		Ohio
PRIVATE	**Industry Standards**	NIST Framework
		CIS Controls
	Financial Industry Controls	PCI DSS
		FINRA Assessment
	Professional Certifications	CISSP
	Contractual Duties	Vendor Management
		Insurance Underwriting

A. TRADITIONAL LEGAL FRAMEWORKS

Many statements of the duty of data security derive from formal legal obligations. Some are "sectoral" federal regulations issued by agencies that oversee highly regulated industries, notably including health care and financial services. Others come from general-purpose consumer protection regulators such as the FTC and state attorneys general, who bring enforcement actions and issue guidance materials. Data breach notification requirements create additional incentives for companies to adopt particular security practices. Finally, a number of states—notably including California, Massachusetts, New York, and Ohio—go further in their particularized data security prescriptions. This Section introduces these examples of traditional legal frameworks—seven in all—that impose a duty of data security on data custodians within their purview.

One legal process is conspicuously absent from this list: civil litigation. There are numerous lawsuits about data security, which raise claims under tort, contract, or consumer protection law, among other theories.[27] Courts considering these cases offer hardly any insight into the *content* of the duty of data security, however, because they almost never reach the merits. Beyond the cost of suing, plaintiffs in such cases face many procedural roadblocks.[28] Several Supreme Court decisions are often understood to raise the bar for Article III standing in privacy cases.[29] Because damages for each individual are low, ordinarily these cases must be brought as class actions if they are to be brought at all, and there are obstacles to class certification.[30] Even if they survive standing and class certification challenges, plaintiffs must demonstrate compensable damages under traditional legal doctrines that may fit poorly.[31] Occasional institutional plaintiffs, such as issuer banks that must replace credit or debit cards compromised in a security breach, may have an easier time avoiding these difficulties.[32] Nevertheless, whoever brings the

27. *See, e.g.*, Torres v. Wendy's Co., 195 F. Supp. 3d 1278, 1281 (M.D. Fla. 2016) (dismissing claims under tort, contract, and consumer protection law); *In re* LinkedIn User Privacy Litig., 932 F. Supp. 2d 1089 (N.D. Cal. 2013) (same).

28. *See* Chris Jay Hoofnagle, *FTC Regulation of Cybersecurity and Surveillance*, *in* THE CAMBRIDGE HANDBOOK OF SURVEILLANCE LAW 708, 722–23 (David Gray & Stephen Henderson eds., 2017) [hereinafter Hoofnagle, *Cybersecurity*] (describing reasons for the "plaintiff litigation void" in privacy and data security cases, and arguing that the FTC ought to fill this void); Edward R. McNicholas et al., *The General Legal Landscape for Information Security*, *in* CYBERSECURITY: A PRACTICAL GUIDE, *supra* note 22, at 2-55 to 2-59 (noting issues such as standing, proximate causation, and class certification that prevent many civil suits over data security from reaching the merits).

29. *See* Spokeo, Inc. v. Robins, 136 S. Ct. 1540 (2016); Clapper v. Amnesty Int'l USA, 568 U.S. 398 (2013). For cases where standing was found lacking, see, for example, Beck v. McDonald, 848 F.3d 262, 275–77 (4th Cir. 2017), *cert. denied sub nom.* Beck v. Shulkin, 137 S. Ct. 2307 (2017); Reilly v. Ceridian Corp., 664 F.3d 38 (3d Cir. 2011); and *In re* Zappos.com, Inc., 108 F. Supp. 3d 949 (D. Nev. 2015). For cases that have rejected challenges to Article III standing, see, for example, Attias v. Carefirst, Inc., 865 F.3d 620 (D.C. Cir. 2017) and Remijas v. Neiman Marcus Grp., LLC, 794 F.3d 688 (7th Cir. 2015).

30. *See* FED. R. CIV. P. 23; Rabin, *supra* note 3, at 335 & n.145.

31. *See* Selco Cmty. Credit Union v. Noodles & Co., 267 F. Supp. 3d 1288 (D. Colo. 2017) (denying tort recovery for violation of PCI DSS, *see infra* Part I.B.3, because the economic loss doctrine required use of contract remedies instead); Rabin, *supra* note 3, at 333–36 (concluding generally that difficulties in establishing damages make tort theories inappropriate for data security liability); Solove & Citron, *supra* note 11, at 754–55 (criticizing narrow judicial understanding of compensable harm caused by data breaches).

32. *See, e.g.*, Lone Star Nat'l Bank, N.A. v. Heartland Payment Sys., 729 F.3d 421 (5th Cir. 2013) (denying motion to dismiss suit by issuer banks arising

case, none of these preliminary challenges goes to the merits. Any claims that survive this procedural gauntlet almost invariably settle at that point. Consequently, there is little clear precedent from private lawsuits to help define the substance of the duty of data security.[33] Fortunately, the legislative and (especially) regulatory actions discussed in this Section help to fill that void. If lawsuits reach the merits more frequently in the future, I would expect the common law to borrow its definition of the duty of data security from those frameworks already operating in the law and in private ordering.

Certainly, the seven frameworks discussed in this Section are not the only state or federal laws that articulate a duty of data security. Many states, for example, impose security obligations on health care providers above and beyond those enforced through the Health Insurance Portability and Accountability Act (HIPAA).[34] Regulations under the federal Fair Credit Reporting Act specify requirements for the proper disposal of certain personal data.[35] Rather than claiming to be a comprehensive list, the seven frameworks discussed here are representative examples of the legal approach to the duty of data security.

from data security breach); *In re* Target Corp. Customer Data Sec. Breach Litig., 64 F. Supp. 3d 1304 (D. Minn. 2014) (same).

33. Charlotte Tschider has collected and coded 163 judicial decisions in data breach cases between August 1993 and April 2017. *See* Data Spreadsheets from Charlotte A. Tschider, Jaharis Faculty Fellow in Health Law & Intellectual Prop., DePaul Coll. of Law (Oct. 17, 2018) (on file with author). Less than two dozen of the cases in Tschider's data set could be said to engage in any substantive discussion of the content of the duty of data security. *Id.* Eight of those concerned only claims brought under the Fair and Accurate Credit Transactions Act, which includes extremely narrow responsibilities for handling personal data in very specific circumstances. *See* 15 U.S.C. §§ 1681–1681x (2017). Most of the remaining cases talked only about the threshold issue of whether a duty existed in the circumstances of the case, not what that duty might be. *See, e.g.*, Weinberg v. Advanced Data Processing, Inc., 147 F. Supp. 3d 1359, 1366 (S.D. Fla. 2015); *In re Target Data Breach Litig.*, 64 F. Supp. 3d 1304; Paul v. Providence Health Sys., 273 P.3d 106 (Ore. 2012); Dittman v. UPMC, 154 A.3d 318 (Pa. 2017). No more than a few scattered cases offered any discussion about the substance of the duty, and then mostly by reference to other frameworks discussed in this Article. *See, e.g.*, *Lone Star Nat'l*, 729 F.3d at 423 (accepting that the PCI standards, see *infra* note 169, define the duty of care for entities within the payment card system); *In re* LinkedIn User Privacy Litig., No. 5:12-CV-03088-EJD, 2014 WL 1323713, at *9 (N.D. Cal. Mar. 28, 2014) (refusing to dismiss a pleading that describes defendant's alleged failure to comply with industry standards, including NIST standards, see *infra* note 126).

34. *See, e.g.*, CAL. CIV. CODE § 56.101 (West 2012).

35. *See* 16 C.F.R. pt. 682 (2018).

1. Federal Sectoral Regulation

Some of the best-known data security rules can be found in the Code of Federal Regulations and apply to certain highly regulated industries that handle sensitive personal data.

The U.S. Department of Health and Human Services (HHS) has promulgated data security rules under the authority of HIPAA.[36] Having completed an earlier more general rulemaking about privacy, HHS issued the final HIPAA Security Rule in 2003.[37] The data security rulemaking process at HHS involved extensive consultation with stakeholders and an expert advisory group.[38] The resulting Security Rule affects only certain covered entities: health care providers (such as doctors and hospitals), insurance companies, and clearinghouses that help process insurance claims, along with the "business associates" who process personal data protected by the statute on those entities' behalf.[39]

The HIPAA Security Rule establishes a duty of data security for covered entities and business associates. The general requirements set out expectations that these data custodians "[i]dentify and protect against reasonably anticipated threats to the security or integrity" of information covered by the statute.[40] They must have documented policies and procedures[41] to implement a series of broadly expressed administrative, physical, and technical safeguards.[42] Covered entities must also have written contracts specifying security duties of their business associates.[43] The Security Rule explicitly tailors the extent of obligations to an organization's scale and resources.[44] Data custodians are instructed to consider their size, complexity, infrastructure, and

36. Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, 110 Stat. 1936 (codified in scattered sections of 18, 26, 29, and 42 U.S.C.).

37. Health Insurance Reform: Security Standards, 68 Fed. Reg. 8334 (Feb. 20, 2003) (to be codified at 45 C.F.R. pts. 160, 162, and 164); *see* 45 C.F.R. pts. 160, 164 (2016).

38. *See* David Thaw, *Enlightened Regulatory Capture*, 89 WASH. L. REV. 329 (2014) (describing process incorporating expert advisory group).

39. *See* 45 C.F.R. § 160.102 (2016).

40. *Id.* § 164.306(a).

41. *Id.* § 164.316.

42. *See id.* §§ 164.308, 164.310, 164.312.

43. *See id.* § 164.314.

44. *See Summary of the HIPAA Security Rule*, HHS.GOV, https://www.hhs.gov/hipaa/for-professionals/security/laws-regulations/index.html (last updated July 26, 2013) ("[T]he Security Rule is flexible and scalable to allow covered entities to analyze their own needs and implement solutions appropriate for their

resources, as well as the costs of various precautions and the likelihood and severity of data security mishaps.[45]

HIPAA does not authorize private lawsuits.[46] The HIPAA Security Rule is enforced instead by a regulator, the Office of Civil Rights (OCR) within HHS. OCR generally reaches settlements yielding published resolution agreements, which always require corrective action and may also include fines, sometimes for millions of dollars.[47]

In financial services, the privacy provisions of the Gramm-Leach-Bliley Financial Modernization Act[48] likewise authorized new industry-specific data security regulations. Power over financial services is divided among many different supervisory agencies who are separately responsible for different types of entities such as conventional banks, credit unions, or securities brokers.[49] Five of the agencies that have formal examination duties coordinate their activities through the Federal Financial Institutions Examination Council (FFIEC), which has emphasized cybersecurity in recent years.[50] A larger group of financial regulators cooperated to develop the "Safeguards Rule," imposing almost identical duties of data security upon the institutions they oversee.[51] The Safeguards Rule requires regulated firms to develop and implement a "comprehensive information security program."[52] This program must incorporate five elements: management by dedicated staff, risk assessment (with specified areas for attention), implementation of information controls, supervi-

specific environments.").

45. *See* 45 C.F.R. § 164.306(b)(2).

46. *See* Acara v. Banks, 470 F.3d 569, 572 (5th Cir. 2006).

47. For a compendium of these resolution agreements in both privacy and security cases under HIPAA, see *Resolution Agreements*, HHS.GOV, https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/index.html (last updated Sept. 20, 2018).

48. 15 U.S.C. §§ 6801–6827 (2017).

49. *See* WILLIAM MCGEVERAN, PRIVACY AND DATA PROTECTION LAW 801–02 (2016).

50. *See About the FFIEC*, FED. FIN. INSTITUTES EXAMINATION COUNCIL, https://www.ffiec.gov/about.htm (last updated Aug. 29, 2018); *Cybersecurity Awareness*, FED. FIN. INSTITUTES EXAMINATION COUNCIL, https://www.ffiec.gov/cybersecurity.htm (last updated Nov. 5, 2018).

51. *See, e.g.*, 16 C.F.R. pt. 314 (2018) (the FTC's version of the Safeguards Rule); 17 C.F.R., pt. 248, subpart A (2018) (the Securities and Exchange Commission's version of the Safeguards Rule, also called Regulation S-P).

52. *See* 16 C.F.R. § 314.3.

sion of service providers' security practices, and periodic reevaluation.[53] Data custodians are instructed that these measures should be "appropriate to your size and complexity, the nature and scope of your activities, and the sensitivity of any customer information at issue."[54] The individual regulators handle enforcement within their spheres; like HHS actions, these typically end in consent orders and usually include monetary payments by defendants.[55]

Thus, both the health care and financial services sectors operate under clearly stated frameworks that impose a duty of data security applicable to particular industry players. The specific elements of each framework emphasize programmatic compliance activities based on risk assessment, and both are enforced by a specialized regulator.

2. Consumer Protection Law

Outside of specialized industries such as health care or financial services, consumer protection regulation is the dominant source of private-sector data security law in the United States. This model concerns itself with the integrity of a transaction that involves personal data, forbidding practices that are unfair or that are based on misstatements or deception.[56] Because general-purpose consumer protection law applies to most commercial entities, the data security framework in consumer protection law has a much broader impact than the sectoral frameworks discussed above.

At the federal level, the FTC is the primary consumer protection regulator. Section 5 of its founding statute announces that "unfair or deceptive acts or practices in or affecting commerce, are hereby declared unlawful"[57] and empowers the FTC to take enforcement action against such conduct.[58] The FTC has

53. *See id.* § 314.4.

54. *Id.* § 314.3(a).

55. *See, e.g.*, Dwolla, Inc., CFPB No. 2016-CFPB-0007 (Feb. 27, 2016); R.T. Jones Capital Equities Mgmt., Inc., Investment Advisers Act of 1940 Release No. 4204, 112 SEC Docket 2848 (Sept. 22, 2015).

56. *See* McGeveran, *supra* note 8, at 977–79.

57. 15 U.S.C. § 45(a)(1) (2017).

58. The FTC generally lacks the authority to seek fines for first offenses under its Section 5 authority. *See* CHRIS JAY HOOFNAGLE, FEDERAL TRADE COMMISSION PRIVACY LAW AND POLICY 113–14 (2016) [hereinafter HOOFNAGLE PRIVACY LAW]. Section 5 does not create any private right of action. *See* Jeff Sovern, *Protecting Privacy with Deceptive Trade Practices Legislation*, 69 FORDHAM L. REV. 1305, 1321–22, 1321 n.63 (2001). Thus, at the federal level, enforcement

reoriented its consumer protection mission considerably toward regulation of data privacy in general, and data security in particular, over the last fifteen to twenty years.[59] Its theory of Section 5 liability in data security cases has evolved over time. The earliest actions alleged that poor security practices were deceptive practices when they were contrary to companies' promises of strong security.[60] In recent years, the FTC increasingly relied instead on the "unfairness" prong of Section 5 in security cases.[61] Unfairness is governed by the so-called "three-part test," which requires that an unfair practice "[1] causes or is likely to cause substantial injury to consumers [2] which is not reasonably avoidable by consumers themselves and [3] [is] not outweighed by countervailing benefits to consumers or to competition."[62]

State attorneys general play a parallel role in consumer protection law. Relying primarily on their authority to enforce state statutes against unfair and deceptive acts and practices (UDAP), they engage in investigations, consultations, and enforcement actions related to inadequate data security.[63]

In almost every data security case brought by the FTC, targeted companies reached a settlement agreement resulting in a consent decree where the company admitted no fault but accepted certain conditions.[64] The consent decrees invariably require establishment of an internal data security compliance program.[65] The FTC publishes all its complaints against companies and resulting consent decrees,[66] and these have become required

of consumer protection law is accomplished through FTC action that is primarily remedial. Violations of FTC consent decrees are punishable by fines, but by definition these are subsequent infractions. *See* 16 C.F.R. § 1.98(c); HOOFNAGLE PRIVACY LAW, *supra*, at 115.

59. *See generally* HOOFNAGLE PRIVACY LAW, *supra* note 58; Hoofnagle, *Cybersecurity*, *supra* note 28, at 14–16; Daniel J. Solove & Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, 114 COLUM. L. REV. 583 (2014).

60. *See* Solove & Hartzog, *supra* note 59, at 636–37 (2014); *see, e.g.*, Eli Lilly & Co., 133 F.T.C. 20 (2002), 2002 WL 34482046; Microsoft Corp., 134 F.T.C. 709 (2002), 2002 WL 34463137.

61. *See* FTC v. Wyndham Worldwide Corp., 799 F.3d 236 (3d Cir. 2015); Solove & Hartzog, *supra* note 59, at 643.

62. 15 U.S.C. § 45(n) (2017).

63. *See* Danielle Keats Citron, *The Privacy Policymaking of State Attorneys General*, 92 NOTRE DAME L. REV. 747, 780–82 (2016).

64. *See* McGeveran, *supra* note 8, at 998–99.

65. *See* HOOFNAGLE PRIVACY LAW, *supra* note 58, at 235.

66. *See Cases and Proceedings*, FED. TRADE COMMISSION, https://www.ftc.gov/enforcement/cases-proceedings (last visited Nov. 20, 2018) (providing access to complaints and consent decrees in Section 5 enforcement actions).

reading for privacy professionals seeking to understand this data security framework.[67] State attorneys general use similar enforcement tactics.[68]

In an influential article, Daniel Solove and Woodrow Hartzog compare this developing FTC precedent to common law.[69] The comparison has some force insofar as a series of case-specific adjudications has accumulated over time to form a recognizable framework embodying a duty of data security. There also are many important differences between the FTC's activity and true common law, however. These mutually settled cases involve no adversarial presentation of arguments or truly independent judgment. And while in general the FTC voluntarily remains consistent with its past cases, it is not bound to do so in the same way that common law formally builds on precedent. Nonetheless, Solove and Hartzog are correct that the content of the FTC framework is just as clear, and as flexible, as evolving common law jurisprudence.

At both the federal and state levels, consumer protection regulators self-consciously engage in norm entrepreneurship as well.[70] In part, they do this through their enforcement, because the resulting consent decrees are read by all privacy lawyers. They also issue extensive informal guidance materials that educate regulated entities about legal expectations in a range of privacy areas, including data security.[71] The FTC, for example, has produced a guide for businesses entitled "Start with Security," which focuses on ten essential data security measures.[72] These principles include several types of access control mechanisms and active vendor management.[73] The FTC also hosts a frequently updated website with advice for businesses about data

67. *See* Solove & Hartzog, *supra* note 59, at 606.

68. *See* Citron, *supra* note 63, at 755, 764–65.

69. Solove & Hartzog, *supra* note 59, at 586.

70. *See* Steven Hetcher, *The FTC as Internet Privacy Norm Entrepreneur*, 53 VAND. L. REV. 2041, 2046 (2000); Solove & Hartzog, *supra* note 59.

71. *See* Citron, *supra* note 63, at 759–60; McGeveran, *supra* note 8, at 1001–02.

72. *See* FED. TRADE COMM'N, START WITH SECURITY: A GUIDE FOR BUSINESS (2015) [hereinafter START WITH SECURITY], https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf; *see also Stick with Security*, FED. TRADE COMMISSION, https://www.ftc.gov/tips-advice/business-center/guidance/stick-security-business-blog-series (last updated Oct. 2017) (providing a series of online posts building on the "Start with Security" framework).

73. START WITH SECURITY, *supra* note 72, at 3.

security compliance.[74] Such "soft law" pronouncements complement consumer protection regulators' enforcement activities. And they are heavily informed by input from the private sector about the best practices already existing on the ground.[75] The combination of enforcement materials and other regulatory guidance provides plenty of information about the nature and content of the duty of data security under consumer protection law.

In several recent cases, targets of FTC data security enforcement actions have argued that the Commission was stretching unfairness authority beyond the bounds allowed by the three-part test.[76] Because this Article focuses on the content of the duty of data security rather than the mechanisms for its enforcement, it will set aside this contentious issue of the FTC's power. The Article does, however, rebut those critics who claim that the FTC's definition of the duty of data security is "unknowable" or lacking a foundation or predictability.[77] Whatever the courts ultimately decide concerning the FTC's power, the content of its data security framework is clear from past enforcement actions and guidance—and, as Part II will show, it is quite consistent with many other frameworks defining the duty of data security. Thus, the *LabMD* court was mistaken to suggest that the content of a data security compliance program is so obscure that the FTC may be unable to require companies to have one. In the end, however, it may not matter terribly much: if the FTC has its wings clipped, state consumer protection regulators will still enforce

74. *Data Security*, FED. TRADE COMMISSION, https://www.ftc.gov/tips-advice/business-center/privacy-and-security/data-security (last visited Nov. 20, 2018); *see also* START WITH SECURITY, *supra* note 72, at 1 ("[T]he FTC has resources to help you think through how those principles apply to your business. There's an online tutorial to help train your employees; publications to address particular data security challenges; and news releases, blog posts, and guidance to help you identify—and possibly prevent—pitfalls.").

75. *See* FED. TRADE COMM'N, PRIVACY & DATA SECURITY UPDATE: 2016, at 12 (2017), https://www.ftc.gov/system/files/documents/reports/privacy-data-security-update-2016/privacy_and_data_security_update_2016_web.pdf (documenting dozens of workshops where the FTC has sought dialogue with industry about privacy and security issues); David Thaw, *The Efficacy of Cybersecurity Regulation*, 30 GA. ST. U. L. REV. 287, 336–42 (2014) (discussing FTC work with industry on data security).

76. LabMd, Inc. v. FTC, 894 F.3d 1221, 1226–27 (11th Cir. 2018); FTC v. Wyndham Worldwide Corp., 799 F.3d 236, 246–47 (3d Cir. 2015); FTC v. D-Link Sys., Inc., No. 3:17-cv-00039-JD, 2017 WL 4150873, at *3–4 (N.D. Cal. Sept. 19, 2017); *see* Hurwitz, *supra* note 10, at 958–59 (arguing that the FTC has exceeded the scope of its authority in privacy and security enforcement).

77. *See supra* notes 3–6 and accompanying text.

their UDAP laws relying on essentially the same duty of data security described in this Article.

3. Data Breach Notification Laws

At the state level, the most pervasive legal response specifically targeting data security challenges has been the spread of breach notification statutes, which require data custodians who have exposed certain personal information to notify the affected data subjects, and sometimes also a regulatory authority. California enacted the first such law in 2003.[78] In just fifteen years since then, all fifty states have imitated California and adopted similar requirements.[79] Specialized federal law also requires breach notification, including regulations under HIPAA[80] and the Gramm-Leach-Bliley Act.[81] European Union regulators included a similar notification requirement in new data protection rules that came into force there in 2018.[82]

Breach notification requirements have driven a large proportion of corporate efforts to improve institutional data security over the last decade or more.[83] A few different considerations contribute to their influence. First and most basically, there are meaningful costs associated with notification itself—postage, public relations consultants, legal advice, identity protection services for potentially disgruntled customers—which can be avoided if breaches are prevented.[84] Furthermore, many lapses

78. *See* CAL. CIV. CODE § 1798.82 (West 2017).

79. For citations to all state breach notification statutes, see *Security Breach Notification Laws*, NAT'L CONF. ST. LEGISLATORS (Sept. 29, 2018), http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx. The District of Columbia, Guam, Puerto Rico, and the U.S. Virgin Islands also have similar statutes. *See id.* The last three states that had not passed such laws—Alabama, New Mexico, and South Dakota—did so in 2017 and 2018: 2018 S.B. 318, Act No. 396 (Ala. 2018); 2017 H.B. 15, ch. 36 (N.M. 2017); 2018 S.B. 62 (S.D. 2018).

80. *See* 45 C.F.R. §§ 164.400–.404 (2017).

81. *See Interagency Guidelines Establishing Information Security Standards*, 12 C.F.R. pt. 570 app. B.

82. Council Regulation 2016/679, of the European Parliament and of the Council on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation), arts. 33, 34, 2016 O.J. (L 119) 1 (EU) [hereinafter General Data Protection Regulation].

83. *See* BAMBERGER & MULLIGAN, *supra* note 7, at 192–94.

84. *See* KAMALA D. HARRIS, ATTORNEY GENERAL, CALIFORNIA DATA BREACH REPORT (2016) [hereinafter CALIFORNIA REPORT], https://oag.ca.gov/sites/all/files/agweb/pdfs/dbr/2016-data-breach-report.pdf.

in security that might have remained concealed in the past are now exposed to public view, forcing companies to absorb the resulting reputational damage and increasing the risk of legal action by either consumer protection regulators or private litigants.[85] Publicizing breaches might even help create a market for strong data security by informing consumers about companies' failures and giving them the option to take their patronage elsewhere.[86]

There are many differences between various states' notification laws, including such features as their definitions of personal information, the size of breach covered by their requirements, and the deadlines within which notification must be made.[87] For this reason, many have advocated for a uniform national breach notification law.[88] However, none of these discrepancies concerns the content of the duty of data security. On that, breach notification laws are consistent. For example, every state excludes effectively encrypted data from the scope of notification responsibilities.[89] In response, companies are more likely to take those precautions, and data security improves as a result. These incentives to avoid notification requirements form a framework of their own.

4. State Data Security Regulation

Finally, some states have moved beyond notification mandates to impose other particular data security obligations. These may or may not be sectoral, although each is limited by the jurisdiction of the state government. Most codify general reasonableness standards, but several provide some additional detail

85. *See* Citron, *supra* note 63, at 767–69.

86. *See* Rabin, *supra* note 3, at 323.

87. *See* PERKINS COIE, SECURITY BREACH NOTIFICATION CHART (2018), https://www.perkinscoie.com/images/content/1/9/v2/197566/Security-Breach-Notification-Law-Chart-June-2018.pdf.

88. *See* Jacqueline May Tom, *A Simple Compromise: The Need for a Federal Data Breach Notification Law*, 84 ST. JOHN'S L. REV. 1569, 1571–72 (2010); Morgan Chalfont, *GOP Chairman Backs National Data Breach Notification Standard*, THE HILL (Oct. 5, 2017), https://thehill.com/policy/cybersecurity/354024-gop-chairman-backs-national-data-breach-notification-standard.

89. *See, e.g.*, 815 ILL. COMP. STAT. 530/5 (2006) (defining "personal information" to exclude encrypted data in most circumstances); MICH. COMP. LAWS § 445.72(1)(a) (2005) (limiting data covered by breach notification duties to "unencrypted and unredacted personal information" or encrypted data compromised with its key); N.C. GEN. STAT. § 75-61(14) (2005) (defining "security breach" to encompass only unencrypted data or encrypted data compromised with its key).

about the duty of data security. This Section will focus on three representative types of state laws: those based on administrative agency regulations in states like Massachusetts and New York; those based on regulatory interpretation of broad statutory language such as California's law; and a new model, seen in Ohio, of creating statutory protection from liability for demonstrating reasonable data security. Several other states have enacted data security legislation.[90] These three categories show three different approaches, but in the end they are more notable for their similarities than for their differences.

The first type of state law resembles the programmatic requirements found in federal regulation of data custodians in the health care and financial services sectors.[91] The Massachusetts Legislature was a pioneer in authorizing the state's regulators to develop a data security framework that went beyond UDAP enforcement or data breach notification incentives.[92] The Massachusetts Department of Consumer Affairs and Business Regulation issued the resulting regulations, which became effective in 2010.[93] The rules apply to "all persons that own or license personal information about a resident," no matter the industry sector.[94] Those custodians must "develop, implement, and maintain a comprehensive information security program"[95] that includes ten specified elements.[96] A Massachusetts regulatory agency has distilled these requirements into a compliance checklist[97] and issued an "FAQ" document[98] to help businesses understand their obligations. These mandates, and the accompanying guidance

90. For examples of state security statutes beyond those discussed in the text, see, for example, CONN. GEN. STAT. § 42-471 (2008) (Connecticut); MD. CODE ANN., COM. LAW § 14-3501 (2018) (Maryland); NEV. REV. STAT. § 603A.210 (2006) (Nevada); OR. REV. STAT. § 646A.622 (Oregon); TEX. BUS. & COM. CODE ANN. § 521.053 (2009) (Texas).

91. *See supra* Part I.A.1.

92. MASS. GEN. LAWS ch. 93H, § 2 (2007).

93. 201 MASS. CODE REGS. 17.00 (2018).

94. *Id.* at 17.01(2).

95. *Id.* at 17.03(1).

96. *Id.* at 17.03(2).

97. MASS. OFFICE OF CONSUMER AFFAIRS & BUS. REGULATION, 201 CMR 17.00 COMPLIANCE CHECKLIST (2018), https://www.mass.gov/files/documents/2018/11/15/compliance-checklist.pdf.

98. MASS. OFFICE OF CONSUMER AFFAIRS & BUS. REGULATION, FREQUENTLY ASKED QUESTIONS REGARDING 201 CMR 17.00 (2018), https://www.mass.gov/files/documents/2018/03/21/201%20CMR%2017%20FAQs%202018_3.pdf.

from regulators, function as a data security framework that potentially affects any entity conducting businesses in Massachusetts.

In 2017, the New York Department of Financial Services promulgated a new set of detailed cybersecurity regulations for financial services.[99] Like the federal financial services rules, these regulations are sectoral, but their coverage is somewhat broader, applying to all entities regulated by "the Banking Law, the Insurance Law or the Financial Services Law."[100] The resulting scope includes banks, trust companies, insurance companies, investment companies, brokers, and mortgage lenders, among others, thus affecting most national financial services firms because of their extensive New York operations.[101] Such broad coverage attracted a lot of notice to the measure. The original rules proposed in 2016 were hotly criticized by many in the industry for being inflexible and overly prescriptive; in response, the regulators reopened the comment period and substantially revised the rules before they took effect, so that they now embody a risk-based approach and provide alternative modes of compliance, such as the use of security subcontractors.[102] Data custodians covered by the revised regulations must name a CISO,[103] conduct periodic risk assessments,[104] engage in annual penetration testing,[105] and configure their networks to protect personal data from unauthorized access.[106] In particular situations such as controlling external access, specific technical measures such as

99. N.Y. COMP. CODES R. & REGS. tit. 23, § 500.00 (2018).

100. *Id.* § 500.01(c).

101. John Zorabedian, *FAQs About the New York DFS Cybersecurity Regulation*, VERACODE (Jan. 3, 2017), https://www.veracode.com/blog/security-news/faqs-about-new-york-dfs-cybersecurity-regulation. Some very small entities are exempt. *See* N.Y. COMP. CODES R. & REGS. tit. 23, § 500.19(a) (exempting entities with fewer than ten employees, less than $5 million a year in gross revenue from New York business operations in each of the last three years, or less than $10 million in total year-end assets including affiliates' assets).

102. *See* Gloria Gonzalez, *New York Cyber Security Law Serves as a Model*, BUS. INS. (Feb. 28, 2017), https://www.businessinsurance.com/article/20170228/NEWS06/912312110/New-York-state-cyber-security-law-serves-as-model; George Lynch, *N.Y.'s Landmark Financial Cybersecurity Rule Takes Effect*, BLOOMBERG BNA (Mar. 8, 2017), https://www.bna.com/nys-landmark-financial-n57982084948.

103. N.Y. COMP. CODES R. & REGS. tit. 23, § 500.04(a).

104. *Id.* § 500.09 (requiring that risk assessment evaluate confidentiality, system integrity, security, and availability of data).

105. *Id.* § 500.05.

106. *Id.* § 500.12.

encryption[107] or multifactor authentication[108] may be mandatory.

The programmatic regulatory model followed in Massachusetts and New York requires companies to engage in assessment, planning, and management to fulfill the duty of data security.[109] California has taken a different approach. Although the state garnered a lot of attention for the novel requirements in a demanding consumer privacy statute enacted in 2018,[110] its somewhat older data security provisions are less directive.

California statutory law requires all businesses to "implement and maintain reasonable security procedures and practices" for the handling of personal information about California residents.[111] Rather than promulgating formal regulations as Massachusetts and New York did, the California Attorney General published a detailed narrative report in 2016.[112] The California Report included recommendations for companies to satisfy their duty of data security under the broadly worded statute.[113] Among these, it incorporated the Center for Internet Security's Critical Security Controls[114] as guidance for what "reasonable" data security entails.[115] These strong signals about

107. *Id.* § 500.15(a) (requiring that entities "implement controls, including encryption, to protect Nonpublic Information held or transmitted by the Covered Entity both in transit over external networks and at rest").

108. *Id.* § 500.12(b) (requiring multifactor authentication for individuals accessing internal networks from an external network unless the CISO approves another method).

109. Oregon's statute spells out an alternative framework very similar to the Massachusetts regulations. *See* OR. REV. STAT. § 646A.622 (2018). It requires a company to implement "reasonable safeguards to protect the security, confidentiality and integrity of the personal information" and specifies several different alternative frameworks a data custodian may use to comply, including HIPAA and Gramm-Leach-Bliley. *Id.*

110. CAL. CIV. CODE § 1798.100 (West 2018) (effective Jan. 1, 2020). This statute creates notice requirements and consumer rights connected to authorized data use, but says nothing about security of data against unauthorized uses. *See supra* notes 19–23 and accompanying text (differentiating data security from other forms of privacy and from cybersecurity).

111. CAL. CIV. CODE § 1798.81.5(b).

112. CALIFORNIA REPORT, *supra* note 84. In contrast, the new California law does empower the Attorney General to promulgate regulations to enforce the provisions of that law. CAL. CIV. CODE § 1798.185.

113. CALIFORNIA REPORT, *supra* note 84, at 27–38.

114. CTR. FOR INTERNET SEC., THE CIS CONTROLS (version 7 2018) [hereinafter CIS CONTROLS], https://www.cisecurity.org/controls/ (allowing access by clicking "Download all CIS Controls (PDF)"). *See generally infra* notes 148–63 and accompanying text (discussing CIS Controls in greater detail).

115. *See* CALIFORNIA REPORT, *supra* note 84, at 30–34.

the expectations of the regulator that is empowered to enforce California's statute qualify as another data security framework. Overall, the California data security regime operates more like the consumer protection frameworks that give the FTC and state attorneys general regulatory discretion,[116] but anchored here in the state's statutory requirement of "reasonable" procedures and practices.

Ohio recently enacted yet another species of state data security law, and this one bears the strongest resemblance to the encryption safe harbors under state breach notification laws.[117] Like them, the statute offers the incentive of escape from a legal penalty as inducement to improve data security. The Ohio statute creates an affirmative defense in tort cases arising from breaches if a data custodian complied with one of a range of listed frameworks for data security.[118] Many of the frameworks on the list can be found elsewhere in this Article, including the HIPAA Security Rule, the CIS Controls, the NIST framework, and the PCI-DSS.[119] In addition, the Ohio statute specifically requires a data custodian to develop and comply with a written security plan designed to provide certain protections, and to scale those protections to the resources and risk of the organization.[120] In short, the Ohio statute purports to offer an affirmative defense for fulfilling the duty of data security as articulated repeatedly in the other thirteen frameworks discussed in this Article. Thus it appears this "affirmative defense" does little more than embody the arguments a data custodian would make against a plaintiff's burden to prove negligence[121] (in the unlikely event that such a tort suit got to the merits at all).[122]

The three forms of state security law each resemble other legal frameworks for the duty of data security discussed in this section. Massachusetts and New York promulgated written regulations similar to the HIPAA Security Rule and the Safeguards

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

117. *See supra* Part I.A.3.

118. OHIO REV. CODE § 1354.01 (2018).

119. *See id.* § 1354.03.

120. *Id.* § 1354.02.

121. *Cf.* KP Permanent Make-Up, Inc. v. Lasting Impression I, Inc., 543 U.S. 111, 120 (2004) ("[I]t would make no sense to give the defendant a defense of showing affirmatively that the plaintiff cannot succeed in proving some element . . . all the defendant needs to do is to leave the factfinder unpersuaded that the plaintiff has carried its own burden on that point.").

122. *See supra* notes 27–33 and accompanying text.

Rule; California embraces flexible enforcement and regulatory guidance, similar to the model under consumer protection law; Ohio provides special protection from liability as an incentive to improve security, just as the data breach notification statutes do. In addition, all the state laws, and indeed all the legal frameworks discussed in Part I.A, draw extensively on industry-based standards as the measure of reasonable compliance. And that provides a cue for this Article to turn to those frameworks that emerge from private ordering—many of them invoked by name in, for example, FTC consent decrees, the California Report, and the Ohio statute.

B. PRIVATE ORDERING FRAMEWORKS

The frameworks described in Section A were all propounded by legislators or (more often) regulators for the purpose of changing behavior. These policymakers sought and received input and comments from the private sector, and especially data custodians themselves, but the rules were nonetheless created through formal legal processes such as legislation, rulemaking, or adjudication.

This Section turns to private ordering—frameworks crafted primarily or entirely by industry, from the bottom up, rather than by government, from the top down. The terminology of "private ordering" is often problematically imprecise.[123] Here I am not invoking Robert Ellickson's iconic Shasta County cattle ranchers,[124] or even Lawrence Lessig's norms, markets, and architecture.[125] In this Article, private ordering refers to the development of an understanding, chiefly within private industry, of sound data security practices, which may then take on the force of law by various means. This privately generated duty of data security might become a set of enforceable legal obligations, for example, by being subsequently embraced by regulators, by getting included in contracts, or by defining eligibility for private designations like industry certifications or professional licenses

123. Steven L. Schwarcz, *Private Ordering*, 97 NW. U. L. REV. 319, 323 (2002) (critiquing "amorphous generalities" found in scholarship that discusses private ordering).

124. ROBERT C. ELLICKSON, ORDER WITHOUT LAW: HOW NEIGHBORS SETTLE DISPUTES (1991) (using interactions between residents of Shasta County, California as a case study on nonlegal dispute resolution systems).

125. LAWRENCE LESSIG, CODE AND OTHER LAWS OF CYBERSPACE (1999) (describing the modalities other than law that shape online conduct).

(which then gain legal recognition through instruments like consent decrees or regulations).

Here again, I will offer seven examples, which include broad industry standards for data security, narrower rules in the financial services sector, best practices established by certification programs for data security professionals, and contractual obligations of data security negotiated between private organizations. They are combined into a few groups for ease of presentation.

1. Industry Standards

Voluntary technical standards proliferate in the data security field, as they do in many complex subject areas. None is itself a legal mandate, but many have been incorporated into legal duties of data security. This Section highlights two frameworks that have become especially prominent, and which are representative of a host of others like them.

Probably the best known industry-based standard is a "Cybersecurity Framework" released by the National Institute of Standards and Technology (NIST).[126] While NIST is actually the federal government's standard-setting agency, in this instance it operated simply as a convener, gathering representatives of industry, academia, and government.[127] President Obama issued an executive order in 2013 directing NIST to oversee development of the framework in collaboration with key stakeholders,

126. NAT'L INST. OF STANDARDS & TECH., FRAMEWORK FOR IMPROVING CRITICAL INFRASTRUCTURE CYBERSECURITY (version 1.1 2018) [hereinafter NIST FRAMEWORK], https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf. This version is a modest revision and update from earlier drafts, and replaces the original NIST Framework promulgated in 2014. Press Release, Nat'l Inst. of Standards & Tech., NIST Releases Version 1.1 of Its Popular Cybersecurity Framework (Apr. 16, 2018), https://www.nist.gov/news-events/news/2018/04/nist-releases-version-11-its-popular-cybersecurity-framework.

127. *See* NAT'L INST. OF STANDARDS & TECH., NIST THREE YEAR PROGRAMMATIC PLAN 2017–2019, at 15 (2017), https://www.nist.gov/sites/default/files/documents/director/planning/3_year_plan_2017-19_web_ready2.pdf ("NIST is increasingly partnering with academic, industrial, and governmental institutions. . . . NIST has the unique convening power and technical independence to help bring those participants together."); *Cybersecurity Framework Frequently Asked Questions*, NIST, https://www.nist.gov/cyberframework/cybersecurity-framework-faqs-framework-basics#developed (last visited Nov. 20, 2018) ("The Framework was developed in a year-long, collaborative process in which NIST served as a convener for industry, academia, and government stakeholders. That took place via workshops, extensive outreach and consultation, and a public comment process.").

particularly private entities involved in the nation's critical infrastructure.[128] Congress later confirmed this approach in statute.[129]

Although most private actors are not legally obliged to follow the NIST Framework, it has proven highly influential, even among institutions far removed from any role in critical infrastructure.[130] President Trump subsequently issued an executive order directing all federal agencies to use the NIST Framework.[131] Regulators such as the FTC frequently invoke the NIST Framework in their informal guidance.[132] Experts have suggested that the FTC may incorporate it more directly into formal regulatory actions in the wake of the *LabMD* decision, which may require more specific injunctions.[133]

The NIST Framework relies heavily upon five privately developed voluntary standards—including the ISO/IEC 27000 family of standards for information security management systems,[134] the COBIT 5 standard from ISACA,[135] and several

128. Exec. Order No. 13,636 § 8, 78 Fed. Reg. 11,739, 11,741 (Feb. 12, 2013).

129. 15 U.S.C. § 272(e)(1) (2017) (instructing NIST to use a consultative process and incorporate industry best practices in developing a "prioritized, flexible, repeatable, performance-based, and cost-effective approach, including information security measures and controls, that may be voluntarily adopted").

130. *See* Justin (Gus) Hurwitz, *Cyberensuring Security*, 49 CONN. L. REV. 1495, 1504–05 (2017) (characterizing the NIST Framework as the "gold-standard" model for cybersecurity and describing its process-based philosophy).

131. Exec. Order No. 13,800 § 1(c)(ii), 82 Fed. Reg. 22,391, 22,391–93 (May 11, 2017).

132. *See, e.g.*, Andrea Arias, *The NIST Cybersecurity Framework and the FTC*, FTC: BUS. BLOG (Aug. 31, 2016, 2:34 PM), https://www.ftc.gov/news-events/blogs/business-blog/2016/08/nist-cybersecurity-framework-ftc ("From the perspective of the staff of the Federal Trade Commission, NIST's Cybersecurity Framework is consistent with the process-based approach that the FTC has followed since the late 1990s, the 60+ law enforcement actions the FTC has brought to date, and the agency's educational messages to companies, including its recent Start with Security guidance.").

133. *See* Timothy J. Muris et al., *11th Circuit Vacates LabMD Enforcement Order; Casts Doubt on Decades of FTC Cybersecurity Enforcement Practices*, SIDLEY AUSTIN: DATA MATTERS (June 12, 2018), https://datamatters.sidley.com/11th-circuit-vacates-labmd-enforcement-order-casts-doubt-on-decades-of-ftc-cybersecurity-enforcement-practices.

134. *See ISO/IEC 27000 Family – Information Security Management Systems*, INT'L ORG. FOR STANDARDIZATION, https://www.iso.org/isoiec-27001-information-security.html (last visited Nov. 20, 2018).

135. *See COBIT 5*, ISACA, https://cobitonline.isaca.org (last visited Nov. 20, 2018).

ANSI/ISA standards[136]—which it designates "informative references."[137] It centers on high-level organizing principles for data security, to be used in conjunction with these informative references and other data security risk management tools.[138]

The NIST Framework breaks down cybersecurity measures into five phases: "Identify, Protect, Detect, Respond, Recover."[139] A comprehensive taxonomy of more specific categories and subcategories provides detail about each of these functions. So, for example, categories under "Protect" include "Access Control," "Awareness and Training," and "Protective Technology."[140] Subcategories under "Access Control," in turn, include that "[i]dentities and credentials are . . . managed . . . for authorized devices [and] users" and that "[p]hysical access to assets is managed and protected."[141] Alongside these numerous branching trees, which organize and describe fundamental data security measures, the NIST Framework also presents four "Implementation Tiers" to characterize different degrees of institutional emphasis on data security risk management.[142] The entire taxonomy is technology-neutral.[143]

The NIST Framework's methodology represents a risk-driven and process-based management approach, with flexibility for a data custodian to use the Framework in a manner that best suits its "business requirements, risk tolerance, and resources."[144] The four tiers may seem to represent degrees of inferiority beneath the most involved, "Adaptive" tier.[145] But the Framework resolutely resists this characterization: "Tiers do not represent maturity levels. . . . Progression to higher Tiers is encouraged when a cost-benefit analysis indicates a feasible and cost-effective reduction of cybersecurity risk."[146] Rather, the

136. *See* ISA, THE 62443 SERIES OF STANDARDS (2016). For a fact sheet about the ISA 62443 series of standards, see ISA, THE 62443 SERIES OF STANDARDS (2016), https://cdn2.hubspot.net/hubfs/3415072/Resources/The%2062443%20Series%20of%20Standards.pdf.

137. NIST FRAMEWORK, *supra* note 126, at 35.

138. *See id.* at 4 ("The Framework complements, and does not replace, an organization's risk management process and cybersecurity program.").

139. *Id.* at 8–9.

140. *Id.* at 7.

141. *Id.* at 29.

142. *Id.* at 8–11.

143. *Id.* at 2.

144. *Id.* at 11.

145. *Id.* at 9–11.

146. *Id.* at 8.

Framework recommends that organizations create two "profiles"—one to represent the categories and subcategories that are being achieved by existing data security practices, and another "target profile" to describe goals for an improved security program—as a process to prioritize next steps in a way that is "driven by the organization's business needs and risk management processes."[147]

Another influential data security framework is the Center for Internet Security's Controls (the CIS Controls).[148] The CIS Controls, originally dating to 2008, are among the previously existing standards incorporated into the NIST Framework as informative references.[149] They were also central to the California Attorney General's recommendations concerning the duty of data security.[150] CIS has boasted of their ability to integrate easily with other frameworks, and even created a chart mapping the relationship between individual aspects of the Controls and other industry standards (including the NIST Framework).[151] The California Attorney General concluded that many of the 657 security breaches it studied could have been prevented or ameliorated through implementation of the CIS Controls.[152]

The CIS Controls consist of twenty recommended data security practices.[153] On the whole, these twenty "prioritized, well-vetted, and supported security" CIS Controls are more precise and technically oriented than the comparatively abstract items in the NIST Framework.[154] The CIS Controls explain why each of the twenty recommended practices are "critical."[155] Each control is further demonstrated by multiple "sub-controls" that offer more detail about steps toward achievement of the stated con-

147. *Id.* at 11.

148. *See* CIS CONTROLS, *supra* note 114.

149. *See* NIST FRAMEWORK, *supra* note 126, at 24–44. Until recently, these were known as the "CIS Critical Security Controls." *See* CTR. FOR INTERNET SEC., THE CIS CRITICAL SECURITY CONTROLS FOR EFFECTIVE CYBER DEFENSE (version 6.1 2016) [hereinafter 2016 CIS CONTROLS]. In addition to the simpler and more inclusive name, CIS made some other incremental changes between the 2016 and 2018 versions.

150. *See* CALIFORNIA REPORT, *supra* note 84, at 30–34; *supra* notes 111–15115 and accompanying text (citing 2016 CIS CONTROLS, *supra* note 149).

151. *See* 2016 CIS CONTROLS, *supra* note 149, at 78–79.

152. *See* CALIFORNIA REPORT, *supra* note 84, at 32.

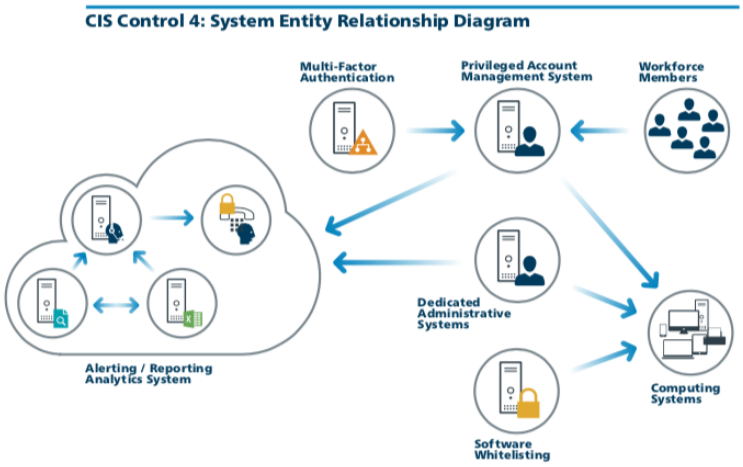
153. CIS CONTROLS, *supra* note 114, at 6–54.

154. *Id.* at 3.

155. *Id.*

trol, particular "procedures and tools" that can assist in implementing and automating it, and a schematic diagram of the relationships between different components of the control.[156]

For example, CIS Control 4, "Controlled Use of Administrative Privileges," begins by explaining two common methods attackers use to exploit sloppily-managed administrative privileges.[157] It then lists nine detailed sub-controls that call for actions such as limiting the employees and devices that have the capacity to alter the system or gain access to other accounts; requiring that those employees use separate credentials for ordinary login and administrator access; and securing administrator access through means such as strong passwords and multifactor authentication.[158] After that, CIS Control 4 moves on to discuss specific technical methods for controlling administrator access, such as running automated scripts to ensure that system administrators are using their administrative credentials only for appropriate purposes, and configuring built-in operating system settings to maximize password strength.[159] Finally, it concludes with this "System Entity Relationship Diagram" for CIS Control 4[160]:



156. *Id.* at 4.
157. *Id.* at 13.
158. *Id.* at 14.
159. *See id.* at 15.
160. *Id.*

The CIS Controls are designed to be modular—an organization can implement a few at a time, improving continuously, depending on its particular risk profile. To facilitate gradual completion, the controls are prioritized: the first six are the most critical aspects of "Cyber Hygiene," constituting "the basic things that you must do to create a strong foundation for your defense."[161] These encompass inventories of hardware, software, and connected devices, continual auditing and reassessment to detect newly identified vulnerability, and the aforementioned control of administrative privileges.[162] CIS suggests that implementation of these controls will "eliminate the vast majority of your organization's vulnerabilities."[163]

The NIST Framework and the CIS Controls each refer to the other, and both are also consistent with a plethora of other independent industry standards.[164] The peaceful coexistence of many standards underscores the broad consensus among security experts about the core elements of the duty of data security. We will use these two as our representative examples and move on to other frameworks that come from private ordering.

2. Financial Industry Controls

The NIST Framework and the CIS Controls discussed in the previous subsection were technology-neutral and applicable to any data custodian in any industry.[165] As we saw in Section A, some heavily regulated industries, notably health care and financial services, have their own legal data security frameworks more tailored to their circumstances.[166] The same is true of non-legal frameworks. Financial transactions often involve specialized articulations of the duty of data security. This subsection

161. *Id.* at 3.

162. *Id.* at 6–23. A previous version of the CIS Controls summarized these high-priority items in less technical terms, as "Count, Configure, Control, Patch, Repeat." 2016 CIS CONTROLS, *supra* note 149, at 80.

163. *See* Kristopher Peterson, *The Top 5 Critical Internet Security Controls Your Company Must Have*, BLUM SHAPIRO (July 3, 2017), http://www.blumshapiro.com/kbarticle/the-top-5-critical-internet-security-controls-your-company-must-have.

164. *See, e.g.*, CIS CONTROLS, *supra* note 114, at 17; NIST FRAMEWORK, *supra* note 126, at 44.

165. The NIST Framework was originally designed with "critical infrastructure" in mind, but that was defined capaciously and the Framework has been applied frequently outside those specialized sectors. *See* NIST FRAMEWORK, *supra* note 126, at v–vi.

166. *See supra* Part I.A.1.

considers two examples. They are representative of private frameworks with a focus on particular technologies or use cases.[167]

Very early in the age of e-commerce, the major credit card brands began including rules about data security measures in the web of contracts among vendors, banks, payment processors, and other actors that operate behind the scenes every time we pay with plastic.[168] These ultimately evolved into the Payment Card Industry Data Security Standard (PCI DSS).[169] The standard is managed by the PCI Security Standards Council, an industry organization governed by five major payment card companies.[170] The Council also sponsors an elaborate program to train and certify experts who are qualified to conduct formal assessments of PCI DSS compliance, and approves hardware and software for use in payment card transactions consistent with the standards.[171]

Because PCI standards are included in contracts establishing payment card procedures, they have legal force over companies participating in that system.[172] (Enforcement complications do arise, however, when companies that are not in direct contractual privity litigate to enforce the PCI standards.[173]) A few

167. A "use case" is basically the computer engineer's equivalent of an attorney's "fact pattern." *See, e.g.*, *Defining Use Cases*, IBM (June 7, 2018), https://www.ibm.com/support/knowledgecenter/en/SSWSR9_11.6.0/com.ibm.pim.dev.doc/pim_tsk_arc_definingusecases.html.

168. *See generally* MCGEVERAN, *supra* note 49, at 415–21.

169. *See* PCI SEC. STANDARDS COUNCIL, PAYMENT CARD INDUSTRY (PCI) DATA SECURITY STANDARD (version 3.2.1 2018) [hereinafter PCI DSS]. PCI documents can be downloaded at https://www.pcisecuritystandards.org/document_library (last visited Nov. 20, 2018).

170. *See PCI Security*, PCI SECURITY STANDARDS COUNCIL, https://www.pcisecuritystandards.org/pci_security (last visited Nov. 20, 2018).

171. *See Program Training & Qualification*, PCI SECURITY STANDARDS COUNCIL, https://www.pcisecuritystandards.org/program_training_and_qualification (last visited Nov. 20, 2018).

172. *See* MCGEVERAN, *supra* note 49, at 417.

173. Issuer banks that must replace payment cards compromised by security breaches sometimes sue defendants whom they allege are responsible for the breach, but when the issuer banks are not parties to the same contracts as the defendants, courts are split on their ability to do so. *Compare, e.g.*, Lone Star Nat'l Bank, N.A. v. Heartland Payment Sys., 729 F.3d 421, 423 (5th Cir. 2013) (holding that the economic loss doctrine did not bar an issuer bank's suit against a payment processor), *with* SELCO Cmty. Credit Union v. Noodles & Co., 267 F. Supp. 3d 1288, 1297 (D. Colo. 2017) (finding that the economic loss doctrine barred suit by an issuer bank against a merchant).

states have incorporated PCI requirements into their law.[174] But the more common governmental response is typified by California Governor Arnold Schwarzenegger, who in 2007 vetoed a bill that would have codified payment card security rules under state law; thanks to the PCI standards, he said, "the marketplace has already assigned responsibilities and liabilities that provide for the protection of consumers."[175]

The rules cover only a single type of transaction that uses predictable types of technology, allowing the PCI DSS to be somewhat more explicit and directive than other frameworks discussed in this Part. The standards are expressed in three levels of increasing complexity. The first level articulates basic principles, the second enumerates steps to meet that requirement, and the most technical layer identifies specific technological means to meet the requirements. For example, Requirement 1 is the installation and maintenance of a firewall system; nested beneath it, Requirement 1.3 is the prohibition of direct access from the internet to system components, and Requirement 1.3.3 instructs data custodians to "[i]mplement anti-spoofing measures to detect and block forged source IP addresses from entering the network."[176] For every element at every level, the PCI DSS provides testing procedures and guidance.

Payment card brands contractually require annual certifications of compliance by participants in their payment card system; smaller entities may conduct self-assessments and periodic scanning, while some larger ones must arrange for professional examinations by qualified outside consultants.[177] These requirements create a duty of data security for every data custodian within the payment card system.

174. *See* MINN. STAT. § 325E.64 (2018); NEV. REV. STAT. § 603A.215 (2018); WASH. REV. CODE § 19.255.020 (2018).

175. *See* Ryan Paul, *Gov. Schwarzenegger Says "Hasta La Vista" to California Data Protection Law*, ARS TECHNICA (Oct. 16, 2007), https://arstechnica.com/security/2007/10/governator-terminates-california-data-protection-law.

176. *See* PCI DSS, *supra* note 169, at 20–25.

177. *See FAQ: How Do I Determine Whether My Business Would Be Required to Conduct an Independent Assessment or a Self-Assessment?*, PCI SECURITY STANDARDS COUNCIL (Feb. 2008), https://pcissc.secure.force.com/faq/articles/Frequently_Asked_Question/How-do-I-determine-whether-my-business-would-be-required-to-conduct-an-independent-assessment-or-a-self-assessment; *PCI Merchant Levels 1–4 and Compliance Requirements – VISA & MasterCard*, PCI POL'Y PORTAL, http://pcipolicyportal.com/what-is-pci/merchants (last visited Nov. 20, 2018); *see also* MCGEVERAN, *supra* note 49, at 417.

Another example of a specialized entity that has produced a data security framework is the Financial Industry Regulatory Authority (FINRA), a nonprofit self-regulatory organization that licenses securities brokers.[178] FINRA has increasingly emphasized the importance of data security practices within the securities industry. It conducted a broad investigatory sweep related to cybersecurity in 2014 and issued a detailed 2015 report calling for certain security measures by licensed brokers; these are consistent with SEC requirements under the Safeguards Rule, but are more demanding.[179] In 2016, FINRA produced a user-friendly "checklist," formatted as an Excel spreadsheet, that small firms may use to help comply with both SEC and FINRA data security standards.[180] Notably, the 2015 report draws heavily upon other standards and discusses their role in guiding members' data security practices, specifically including the NIST Framework, the CIS Controls, and the PCI DSS.[181]

Incidentally, the FINRA model is typical of many industries beyond banking and investment that are grappling with data security issues. Whether they have FINRA's authority based in licensure or just their bully pulpit, other professional associations have followed FINRA's lead in providing frameworks for their constituents. For example, the National Association of Insurance Commissioners, the organization that coordinates activities of state insurance regulators, issued a model data security law in late 2017[182] which draws on the New York regulations[183] described previously. Many readers of this Article will relate to another example: the American Bar Association has a cybersecurity task force that has issued a handbook and a vendor

178. *See About FINRA,* FINRA—FIN. INDUSTRY REG. AUTHORITY, https://www.finra.org/about (last visited Nov. 20, 2018).

179. *See* FINRA REPORT, *supra* note 19, at 1–2.

180. *See Small Firm Cybersecurity Checklist*, FINRA—FIN. INDUSTRY REG. AUTHORITY, http://www.finra.org/industry/small-firm-cybersecurity-checklist (last visited Nov. 20, 2018) [hereinafter FINRA Checklist].

181. *See, e.g.*, FINRA REPORT, *supra* note 19, at 8–10; *see also id.* at 42–44 (explaining the NIST Framework in a separate appendix); FINRA Checklist, *supra* note 180 ("This checklist is primarily derived from the National Institute of Standards and Technology (NIST) Cybersecurity Framework and FINRA's Report on Cybersecurity Practices.").

182. NAT'L ASS'N OF INS. COMM'RS, INSURANCE DATA SECURITY MODEL LAW (2017); *see also Cybersecurity*, NAT'L ASS'N INS. COMMISSIONERS, http://www.naic.org/cipr_topics/topic_cyber_risk.htm (last updated July 11, 2018).

183. *See supra* notes 99–108 and accompanying text (discussing New York regulations).

contracting checklist advising attorneys about meeting their special heightened data security responsibilities.[184]

3. Professional Certifications

The private sector has generated a bewildering array of certifications to be earned by security professionals. A majority of professionals in the field hold at least one certification, and certified cybersecurity experts typically earn the highest average salaries in IT.[185] The body of knowledge taught and tested in connection with these certification programs establishes another framework that significantly influences industry practices and constitutes a duty of data security.

An alphabet soup of certifications now offers specialists an opportunity to receive training, pass an exam, and append letters to their name that demonstrate expertise in data security. Certifications are offered by multiple acronym-laden organizations in the security field, such as ISACA,[186] GIAC,[187] and CompTIA,[188] among many others. Admittedly, these varied credentials have not yet gelled into a single professional standard unified across the field of cybersecurity—compared to, say, the professional standards for doctors, lawyers, or accountants. But each of these programs emphasizes fundamental technical and organizational methods, creating a broad professionalized under-

184. AM. BAR ASS'N CYBERSECURITY LEGAL TASK FORCE, VENDOR CONTRACTING PROJECT: CYBERSECURITY CHECKLIST (2017); JILL D. RHODES & VINCENT I. POLLEY, THE ABA CYBERSECURITY HANDBOOK: A RESOURCE FOR ATTORNEYS, LAW FIRMS AND BUSINESS PROFESSIONALS (2013).

185. *See* GLOBAL KNOWLEDGE, *supra* note 18.

186. ISACA (which is known only by its acronym) offers five well-regarded certifications, notably the Certified Information Security Auditor (CISA). *See ISACA Certification: IT Audit, Security, Governance and Risk*, ISACA, http://www.isaca.org/certification/pages/default.aspx (last visited Nov. 20, 2018).

187. GIAC, the Global Information Assurance Certification, actually consists of over thirty specialized data security certifications. *See GIAC Certifications: Categories*, GIAC, https://www.giac.org/certifications/categories (last visited Nov. 20, 2018); *GIAC Information Security Certification – Program Overview*, GIAC, https://www.giac.org/about/program-overview (last visited Nov. 20, 2018).

188. CompTIA, the Computing Technology Industry Association, offers four different series of certifications, each demonstrating increasing levels of knowledge. *See About CompTIA*, COMPTIA, https://certification.comptia.org/about-us (last visited Nov. 20, 2018); *CompTIA Certifications*, COMPTIA, https://certification.comptia.org/certifications (last visited Nov. 20, 2018).

standing of data security duties that has developed organically.[189] Moreover, it continues to evolve and converge as this young field matures.

The closest thing to a dominant professional framework is connected to the Certified Information Systems Security Professional (CISSP), which is overseen by "(ISC)²," an independent nonprofit organization.[190] The CISSP is a more basic or foundational certification, but it also requires minimum years of experience in the field as well as performance on an exam.[191] The FTC favors professionals who hold the CISSP credential for the leadership and evaluation of data security; five recent data security consent decrees listed the CISSP as an acceptable qualification, while no other certification was specified in any more than three of them.[192]

The CISSP exam covers eight topical domains, ranging from "security and risk management," which covers fundamental issues of governance, law, and ethics, to "security engineering," which includes technical information about cryptography and the particular vulnerabilities of different computer memory mechanisms, but also basic physical security matters such as fire prevention.[193] A 1000-plus-page leading study guide for the exam explains in its first few pages how security planning is essential to everything that follows, and must be pursued with engagement of senior management and with sensitivity toward the

189. *See* Thaw, *supra* note 75, at 325 & n.167.

190. *See* Ed Tittel & Kim Lindros, *Best Information Security Certifications 2018*, BUS. NEWS DAILY (Apr. 23, 2018), https://www.businessnewsdaily.com/10708-information-security-certifications.html ("The CISSP continues to be highly sought after by IT professionals and well recognized by IT organizations. It is a regular fixture on most-wanted and must-have security certification surveys."); Michael Warne, *The Value of CISSP in Cybersecurity Leadership*, DIGITAL DOUGHNUT (Jan. 31, 2017), https://www.digitaldoughnut.com/articles/2017/january/the-value-of-cissp-certification-in-cybersecurity (referring to CISSP as a "gold standard" in data security certifications).

191. *See* Tittel & Lindros, *supra* note 190.

192. *See* FTC v. Ruby Corp., No. 1:16-CV-02438 (D.D.C. Dec. 14, 2016), https://www.ftc.gov/system/files/documents/cases/161214ashleymadisonorder1.pdf; *In re* ASUSTeK Computer, Inc., File No. 142-3156, 2016 WL 4128217, at *13 (F.T.C. July 18, 2016); *In re* Fandango, LLC, 2015-1 Trade Cas. (CCH) ¶ 17098, at *7 (Aug. 13, 2014); *In re* Credit Karma, Inc., 2015-1 Trade Cas. (CCH) ¶ 17099, at *7 (Aug. 13, 2014); *In re* Accretive Health, Inc., File No. 122-3077, 2014 WL 726603, at *4 (F.T.C. Feb. 5, 2014).

193. *See* (ISC)², CERTIFIED INFORMATION SYSTEMS SECURITY PROFESSIONAL: CERTIFICATION EXAM OUTLINE (2018); JAMES MICHAEL STEWART ET AL., CERTIFIED INFORMATION SYSTEMS SECURITY PROFESSIONAL STUDY GUIDE xxxiv, xxxix, 223–24, 376–77, 402–06 (7th ed. 2015).

"goals, mission, and objectives of the organization," including cognizance of "a business case, budget restrictions, or scarcity of resources."[194] The model taught to CISSP students is a process-based and risk-conscious approach to security, expressed in terms of both governance and the appropriate technical responses to security threats.

4. Contractual Duties

Practicing privacy lawyers routinely find themselves drafting or negotiating business-to-business contracts that involve transfer of personal data from one custodian to another for functions such as customer service, billing and collection, analytics, and so forth. In these contracts, entities providing the information usually impose a duty of data security on the recipients. We have already seen that the PCI DSS is incorporated into contracts and enforced that way.[195] Some sectoral statutes, including HIPAA[196] and the Gramm-Leach-Bliley Act,[197] require written agreements and spell out terms they must include in order to codify a subcontractor's duty of data security. But private firms outside the scope of such specialized statutes also include similar provisions in data transfer agreements with vendors and other third parties, and they also conduct extensive audits of those service providers to ensure compliance. Some contracts also include indemnification for data security problems, thus engaging in private ordering to apportion the risks of breaches as well as the related duties.

Because these are private individual agreements, one cannot simply look them up in a centralized document as one can with statutes and regulations, or even with voluntary standards like the NIST Framework and CIS Controls. For purposes of this

194. STEWART ET AL., *supra* note 193, at 14–16.

195. *See supra* notes 169–73 and accompanying text.

196. *See* 45 C.F.R. §§ 164.308(b), 164.314(a) (2016) (requiring business associate agreements); *Business Associate Contracts*, HHS.GOV (Jan. 25, 2013), https://www.hhs.gov/hipaa/for-professionals/covered-entities/sample-business-associate-agreement-provisions/index.html (explaining what a business associate agreement is and providing sample contract language).

197. *See* 16 C.F.R. § 314.4(d) (2018) (requiring written contracts to ensure that service providers comply with the Safeguards Rule); Scott & Scott, LLP, *GLBA Compliance Considerations in Technology Transactions*, LEXOLOGY (Jan. 7, 2016), https://www.lexology.com/library/detail.aspx?g=bb806be4-faad-4207-9c6b-47ccb8e96b1d (quoting language for use in subcontracts to comply with the Safeguards Rule).

Article, however, we can turn to two examples of detailed contractual data security mandates. One of them is a privately developed standardized questionnaire for use with vendors and other affiliates; the other is a selection of insurance underwriting requirements.

Oversight of third-party vendors has been a hot topic in data privacy and security.[198] But while general advice and conventional wisdom have been in plentiful supply, there has not been a public standardized methodology to cite as the industry practice in vendor management. In 2016, a number of technology companies formed the Vendor Security Alliance and proposed a standard questionnaire that data custodians could use when evaluating the security practices of potential service providers.[199]

The questions request detailed answers about a lengthy list of topics including, for example: access controls, proactive security measures such as penetration testing and cryptography, incident response protocols, and software supply chain issues.[200] The supporting documentation includes external audits and certifications.[201] These proposals for newly standardized expectations illustrate the data security frameworks that are already embodied in countless contracts between data custodians and their vendors.

The emergence of cybersecurity insurance for businesses that handle personal information has given birth to another cluster of contractual frameworks for the duty of data security.[202] Insurers can and do push their policyholders to adopt practices

198. *See, e.g.*, Leslie T. Thornton et al., *Governing Privacy and Security with Vendors—Contracting with Service Providers*, *in* 6 SUCCESSFUL PARTNERING BETWEEN INSIDE AND OUTSIDE COUNSEL § 82.17 (Robert L. Haig ed., 2018); David Katz, *Contracting in a World of Data Breaches and Insecurity: Managing Third-Party Vendor Engagements*, LEXISNEXIS, https://www.lexisnexis.com/communities/corporatecounselnewsletter/b/newsletter/archive/2013/05/02/contracting-in-a-world-of-data-breaches-and-insecurity-managing-third-party-vendor-engagements.aspx (last visited Nov. 20, 2018).

199. *See* VENDOR SECURITY ALLIANCE, https://www.vendorsecurityalliance.org (last visited Nov. 20, 2018).

200. *See 2018 Questionnaire*, VENDOR SECURITY ALLIANCE (Dec. 22, 2017), https://www.vendorsecurityalliance.org/questionnaire2018.html.

201. *Id.*

202. *See generally* SHACKELFORD, *supra* note 19, at 246–52; Sean Cooney, *Untangling the Mystery of Cybersecurity Insurance*, LAW J. NEWSLETTERS (Feb. 2017), https://www.lawjournalnewsletters.com/sites/lawjournalnewsletters/2017/02/01/untangling-the-mystery-of-cybersecurity-insurance (discussing the wide range of cybersecurity insurance policies that have emerged).

that reduce the insurer's risk of loss—and simultaneously promote better protection of personal data.[203]

For a variety of reasons, companies' standard commercial general liability policies have not been effective means for insuring against the costs of a data breach.[204] In recent years, specialized "cyberliability" insurance against data security losses required high premiums for rather limited coverage, subject to significant conditions and limitations; many data custodians have found it impossible to secure any affordable insurance policies for breaches.[205] The biggest reason for this tight insurance market is the unavailability and unreliability of data about risk of loss that would allow for sound underwriting.[206]

As a result, before writing a policy that includes data security risks, insurers today scrutinize an individual company's data handling practices very carefully and demand adherence to baseline practices as a condition for insurance.[207] The International Association of Privacy Professionals (IAPP) collected the initial application forms used by three leading cybersecurity insurance providers: Ace Group (which recently merged with

203. *See* Hurwitz, *supra* note 130, at 1533 (describing the insurer's role as a "regulator" that tries, through its underwriting process, to "educate and instruct the insured on how to reduce . . . risks"); Kesan & Hayes, *supra* note 3, at 268 ("Insurers are in a unique position to push companies to adopt more consistently secure data-security practices, including encryption, firewalls, intrusion detection systems, and stronger internal controls for data handling.").

204. *See* Kesan & Hayes, *supra* note 3, at 229–31.

205. *See* Jim Finkle, *Cyber Insurance Premiums Rocket After High-Profile Attacks*, REUTERS (Oct. 12, 2015), https://www.reuters.com/article/us-cybersecurity-insurance-insight-idUSKCN0S609M20151012.

206. *See* PWC, TOP ISSUES: THE PROMISE AND PITFALLS OF CYBER INSURANCE 3 (2016) ("The biggest challenge for insurers is that cyber isn't like other risks. There is limited publicly available data on the scale and financial impact of attacks and threats are very rapidly changing and proliferating."); COSTIS TOREGAS & NICOLAS ZAHN, THE GEORGE WASH. UNIV. CYBER SEC. POLICY & RESEARCH INST., INSURANCE FOR CYBER ATTACKS: THE ISSUE OF SETTING PREMIUMS IN CONTEXT (2014) (discussing the challenges that insurers face understanding and quantifying cyber risks); Kesan & Hayes, *supra* note 3, at 218–19 (explaining that insurers' lack of information about both potential policyholders' data security precautions and the nature and scale of risks makes insurance expensive and unpredictable).

207. Eric Nordman, *Managing Cyber Risk*, CIPR NEWSL. (Oct. 2012), https://www.naic.org/cipr_newsletter_archive/vol5_manage_cyber_risk.htm ("Securing a cyber-liability policy will not be a simple task. Insurers writing this coverage will be interested in the risk-management techniques applied by the business to protect its network and its assets.").

Chubb), USLI, and Philadelphia Insurance.[208] All three applications ask detailed questions about the applicant's risk assessment process and testing, its governance of data security, and the use of particular protective measures such as firewalls, encryption, patching, password strength, and multifactor authentication.[209] Policyholders who do not exercise the degree of caution they promised in the underwriting process can find themselves denied coverage in the event of a loss.[210]

A 2016 white paper published by Chubb explained a cyberinsurance underwriting methodology loosely based on the traditional COPE methodology for insuring real property.[211] The white paper suggested that a new "CyberCOPE" would simplify and standardize underwriting and facilitate sharing of risk data.[212] Insurers would assess risk using considerations such as the scale of an applicant's network and the quantity and sensitivity of the data it held, and would also check practices in particular areas including encryption, firewalls, and account access architecture.[213]

The procedural and technological protective measures listed in the applications and the white paper all resemble one another. Together, they create a duty of data security, and powerful incentives to fulfill it, for companies that have invested in cyberinsurance. Moreover, insurers have not contented themselves with simply asking questions about data security and conditioning future coverage on the answers; they are taking an active and ongoing role in risk management and prevention. Shauhin Talesh, a scholar of law and social science, recently completed a study of the cyberinsurance industry based on content analysis

208. *See Sample Cyberinsurance Applications*, IAPP, https://iapp.org/resources/article/sample-cyberinsurance-applications (last visited Nov. 20, 2018).

209. *Id.*

210. *See, e.g.*, Complaint at 11–15, Columbia Cas. Co. v. Cottage Health Sys., No. 15-cv-03432, 2015 WL 4497730 (C.D. Cal. July 17, 2015). The case was dismissed, but only because the defendant successfully asserted mandatory alternative dispute resolution provisions in the insurance contract. *See Columbia Cas. Co.*, 2015 WL 4497730, at *2.

211. RUSS COHEN, CHUBB, CYBERCOPE®: TRANSFORMING CYBER UNDERWRITING 2–3 (2016). COPE stands for "Construction, Occupancy, Protection, and Exposure." *See* Christopher J. Boggs, *Understanding Commercial Property Underwriting and 'COPE'*, INS. J. (Feb. 3, 2015), https://www.insurancejournal.com/news/national/2015/02/03/356085.htm.

212. COHEN, *supra* note 211, at 2–3, 7.

213. *Id.* at 4–6.

of presentations at industry conferences and webinars and interviews with participants at these events.[214] He found that insurers in this space are actively assisting policyholders in fraud detection; providing written manuals and trainings; providing crisis telephone hotlines to assist in incident response; and offering vendor management services.[215]

Moving forward, we can expect insurers will do even more to drive adherence to a predefined duty of data security. Many experts agree that making these insurance policies more affordable—and therefore more widespread—will require better information for insurers to use in making more efficient risk assessments, and more uniform recommendations for what minimum security measures insurers should require of policyholders.[216] In one ongoing project addressing these linked issues, the Department of Homeland Security (DHS) is trying to promote greater information sharing about cybersecurity incidents in the hope that doing so will "foster both the identification of emerging cybersecurity best practices across sectors and the development of new cybersecurity insurance policies that 'reward' businesses for adopting and enforcing those best practices."[217] Those best practices will be molded by the emerging consensus about the duty of data security and will, in turn, contribute to its further development. Even without the participation of DHS, private insurers are already establishing best practices by making minimum data security measures a contractual requirement of coverage.[218]

Private institutional data security recommendations leach into the law in this area, as they always have in other settings.[219] The FTC's reliance on certification standards for quality control in its consent decrees is part of a much broader trend.[220] As noted above, California's Attorney General has specifically embraced

214. Shauhin A. Talesh, *Data Breach, Privacy, and Cyber Insurance: How Insurance Companies Act as "Compliance Managers" for Business*, 43 LAW & SOC. INQUIRY 417, 422–25 (2018) (explaining study methodology).

215. *Id.* at 428–32.

216. *See, e.g.*, Liam M.D. Bailey, *Mitigating Moral Hazard in Cyber-Risk Insurance*, 3 J.L. & CYBER WARFARE 1 (2014) (proposing a "government funded information sharing platform for insurers . . . in an effort to discount premiums for insureds").

217. Dep't of Homeland Sec. Nat'l Prot. & Programs Directorate, *Cybersecurity Insurance*, DEP'T HOMELAND SECURITY (June 30, 2016), https://www.dhs.gov/cybersecurity-insurance.

218. *See supra* note 207 and accompanying text.

219. *See supra* notes 7–8 and accompanying text.

220. *See supra* note 192 and accompanying text.

the privately developed CIS Controls as a route to compliance with the state's legal requirements,[221] and the FTC has invoked the NIST Framework.[222] Ohio included a list of privately developed data security frameworks in the text of its data security safe harbor statute.[223] Contracts impose security obligations on data custodians that are enforceable in court.[224]

More generally, principles held widely among security professionals and private data custodians have begun to shape the duty of data security, both in law and in practice. To name examples of two such concepts: the importance of "security by design" and the rejection of "security by obscurity," or the significance of certain fundamental architectural safeguards such as firewalls and encryption, both originated among security professionals but now permeate all the frameworks, legal and private. The law routinely absorbs industry standards and transforms them into legal duties. That process is well underway in the realm of data security. The next Part will explore in greater detail the convergence of different frameworks on this emerging duty of data security.

II. CONTENT OF THE DUTY OF DATA SECURITY

A synthesis of the fourteen frameworks identifies key features they share. This Part explains how a clear legal duty of data security appears in their converging consensus. First, Section A begins by observing how all the frameworks embrace some form of a reasonableness requirement, whether or not using that name. Section B explores the heavy emphasis in most frameworks on the procedural measures that data custodians should take to improve their compliance structures, such as developing an internal policy appropriate to their risk and training employees about it. Section C then considers the architectural requirements of frameworks, which are usually technologically neutral but identify broad principles that guide responsible design of networks. Finally, Section D looks at the most granular aspects of the frameworks, specifying serious data security errors that must be avoided—what I call "worst practices."

221. *See* CALIFORNIA REPORT, *supra* note 84, at 30; *see also supra* note 115 and accompanying text.

222. *See supra* note 132 and accompanying text.

223. *See supra* note 118.

224. *See, e.g.*, *supra* notes 195–97 and accompanying text.

A. REASONABLENESS AND RISK

All fourteen frameworks are anchored in some evaluation of the security risks faced by data custodians and the reasonable steps they should take in response to those risks. Solove and Hartzog, the privacy scholars responsible for the pathbreaking article synthesizing the FTC's privacy and security jurisprudence,[225] wrote another article which was almost as insightful. Published in the often irreverent legal journal *Green Bag*, it was entitled "The Ultimate Unifying Approach to Complying with All Laws and Regulations."[226] Its entire content: "Be reasonable."[227] They were joking—but not entirely. As they clearly demonstrated in their FTC research, the content of many legal standards can be distilled to overarching rules of reasonableness.

Many of the older legal frameworks analyzed in Part I use the language of reasonableness when describing the duty of data security. FTC complaints define that duty in the negative, by condemning companies for information-handling practices that "failed to provide reasonable security to prevent unauthorized access to personal information on their network."[228] These complaints have alleged that defendant companies did not use basic security safeguards that were comparatively easy to implement, and that this failure exposed personal data that should be considered sensitive in the circumstances. The *LabMD* court assumed, without much basis, that these reasonableness standards were anchored in tort negligence principles.[229] While the

225. *See supra* note 69 and accompanying text.

226. Daniel J. Solove & Woodrow Hartzog, *The Ultimate Unifying Approach to Complying with All Laws and Regulations*, 19 GREEN BAG 2D 223 (2016) ("Be reasonable.").

227. *Id.* (providing an example of an explanatory parenthetical compliant with Bluebook requirements—that truly summarizes the entire source).

228. Complaint ¶ 18, *In re* Uber Techs., Inc., File No. 1523054 (F.T.C. Aug. 15, 2017), https://www.ftc.gov/system/files/documents/cases/1523054_uber_technologies_revised_complaint_0.pdf ("Respondent has engaged in a number of practices that, taken together, failed to provide reasonable security to prevent unauthorized access to Rider and Driver personal information . . . ."); *see also* Complaint ¶ 31, *In re* Ruby Corp., No. 1:16-cv-02438 (D.D.C. Dec. 14, 2016), https://www.ftc.gov/system/files/documents/cases/161214ashleymadisoncmplt1.pdf (bringing complaint against parent company of the infidelity website Ashley Madison); Complaint ¶ 10, *In re* Dave & Buster's, Inc., No. C-4291 (F.T.C. May 20, 2010), https://www.ftc.gov/sites/default/files/documents/cases/2010/06/100608davebusterscmpt.pdf (alleging respondent's "failure to employ reasonable and appropriate security measures to protect personal information").

229. *See* LabMD v. FTC, 894 F.3d 1221, 1231 (11th Cir. 2018) ("The Commission's decision in this case does not explicitly cite the source of the standard

resemblance is evident, and tort law may have been the origin of reasonableness rationales, they have now proliferated so widely through the law of data security (and indeed, the law of everything else) that reference to tort law alone tells a seriously incomplete story. For example, the HIPAA Security Rule emphasizes reasonableness. "Covered entities and business associates may use any security measures that allow the covered entity or business associate to reasonably and appropriately implement the standards and implementation specifications" in the Rule.[230] These determinations must be informed by a thorough risk assessment in accordance with the specification in the Rule.[231] The Ohio data security statute provides its safe harbor to a data custodian whose security plan "reasonably conforms to an industry recognized cybersecurity framework."[232]

Thus, as summarized a few years ago by Peter Sloan, an attorney specializing in information governance, "[t]he notion of reasonableness permeates explicit statutory and regulatory requirements for safeguarding information, and appears to be a central tenet of FTC enforcement orders regarding information security."[233]

---

of unfairness it used . . . . It is apparent to us, though, that the source is the common law of negligence." (citing RESTATEMENT (SECOND) OF TORTS § 281 (AM. LAW INST. 1965))).

230. 45 C.F.R. § 164.306(b)(1) (2017).

231. *Id.* § 164.308(a)(1)(ii)(A) (requiring that covered entities "conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information").

232. OHIO REV. CODE ANN. § 1354.02(A)(1) (West 2018).

233. *See* Peter Sloan, *The Reasonable Information Security Program*, 21 RICH. J.L. & TECH., no. 1, 2014, at 2. Sloan is among those who has identified common threads in data security law in recent years; he names six recommendations for a "reasonable" data security program:

> 1. An organization should identify the types of information in its possession, custody, or control for which it will establish security safeguards ("Protected Information").
>
> 2. An organization should assess anticipated threats, vulnerabilities, and risks to the security of Protected Information.
>
> 3. An organization should establish and maintain appropriate policies and administrative, physical, and technical controls to address the identified threats, vulnerabilities, and risks to the security of Protected Information.
>
> 4. An organization should address the security of Protected Information in its third-party relationships.
>
> 5. An organization should respond to detected breaches of the security of Protected Information.

More recently, some frameworks have moved away from the explicit language of "reasonableness," perhaps in part because of the great discomfort IT professionals and other technically-oriented stakeholders express about that word.[234] However, these frameworks continue the reliance on individualized risk assessment, with the result that they function in almost the same way—because responses shaped by a proper risk assessment are, by definition, reasonable.

The New York regulations, for example, require "each company to assess its specific risk profile and design a program that addresses its risks in a robust fashion."[235] Massachusetts follows a similar path, and regulators there explicitly tie risk to a company's size and resources and the magnitude of the harms that could result from poor data security.[236]

If anything, private ordering calibrates the duty of data security to risk even more emphatically. For example, risk assessment is absolutely central to the NIST Framework, which explains right near the beginning of the document:

> To manage risk, organizations should understand the likelihood that an event will occur and the potential resulting impacts. With this information, organizations can determine the acceptable level of risk for achieving their organizational objectives and can express this as their risk tolerance. With an understanding of risk tolerance, organizations can prioritize cybersecurity activities, enabling organizations to make informed decisions about cybersecurity expenditures.[237]

> 6. An organization should periodically review and update its policies and controls for the security of Protected Information.

Id. at 3–5.

234. For more on this resistance, see *infra* Part III.A.

235. N.Y. COMP. CODES R. & REGS. tit. 23, § 500.00 (2018).

236. *See* MASS. OFFICE OF CONSUMER AFFAIRS & BUS. REGULATION, FREQUENTLY ASKED QUESTIONS REGARDING 201 CMR 17.00, at 3 (2018), https://www.mass.gov/files/documents/2018/03/21/201%20CMR%2017%20FAQs%202018_3.pdf ("The regulation adopts a risk-based approach to information security. A risk-based approach is one that is designed to be flexible while directing businesses to establish a written security program that takes into account the particular business's size, scope of business, amount of resources and the need for security.").

237. NIST FRAMEWORK, *supra* note 126, at 4; *see also id.* at 22–23 (incorporating risk assessment and management into the Framework Core).

FINRA similarly charges data custodians with "selecting controls appropriate to the firm's technology and threat environment."[238] And the Vendor Security Alliance counsels data custodians who are hiring subcontractors that vendors should use controls proportionate to their risk.[239]

Whether expressed through an overarching rule of reasonableness, a requirement to conduct a risk assessment, or both, all fourteen frameworks strike a balance. The considerations taken into account broadly align. They include a data custodian's size and resources, the cost or burden of particular precautions, and the sensitivity of personal data (and thus the risk of harm if it goes astray).[240] This consistent framing explains why legal treatises that consider data security devote entire chapters to risk management principles.[241]

Embedded in all these frameworks is the understanding that larger institutions are held to a more stringent duty of data security. Data custodians also may have different risk profiles based on the privacy sensitivity of the data they hold (e.g. health data); potential for profit through identity theft or other techniques (e.g. account numbers); the numbers of employees and third parties who legitimately need access to the data; retention times; and many more factors. Thus, the data security measures expected of Equifax or a large hospital system will not be the same as those in a small brokerage firm or the neighborhood corner store. Nor will the same duty of data security apply to data custodians who hold only basic information (like names and addresses) and those whose records concern health or finances. In other words, the duty of data security scales up or down in proportion to the resources and risk profile of each data custodian.

238. FINRA REPORT, *supra* note 19, at 16.

239. *2018 Questionnaire*, *supra* note 200.

240. *See, e.g.*, 16 C.F.R. § 314.3(a) (2018) (Safeguards Rule); 45 C.F.R. § 164.306(b)(2) (2016) (HIPAA Security Rule); COHEN, *supra* note 211, at 4–6 (describing underwriting methodologies keyed to the scale and risk exposure of a data custodian seeking insurance for data security losses); *PCI Merchant Levels 1–4 and Compliance Requirements – VISA & MasterCard*, PCI POL'Y PORTAL, http://pcipolicyportal.com/what-is-pci/merchants (last visited Nov. 20, 2018) (listing PCI DSS requirements).

241. *See, e.g.*, Megan Costello, *Corporate Risk Management*, *in* 1 DATA SECURITY AND PRIVACY LAW 217 (Ronald N. Weikers & Megan Costello eds., 2018); Bill Hardin, *Data Protection: Risk Management*, *in* CYBERSECURITY: A PRACTICAL GUIDE, *supra* note 22, at 6-1 to 6-28.

B. SYSTEMS OF COMPLIANCE

The duty of data security requires not only that a data custodian's efforts to protect data be reasonable and appropriate to its resources and level of risk, but also that they be systematic. Many of the fourteen frameworks focus considerably more on the architecture of the custodian's compliance management than on the architecture of digital networks themselves. Thus, for example, the portion of the HIPAA Security Rule concerned with administrative safeguards—management structures such as risk analysis, dedicated security management responsibility, training, and contingency planning—is considerably longer and more detailed than either of the comparable sections laying out physical or technical safeguards.[242]

Many other legal frameworks in Part I compel data custodians to implement formal data security compliance programs; these include the Safeguards Rule and the Massachusetts and New York data security regulations. The California Report concludes that a risk management approach is a "minimum standard of care for personal information"[243] which "means organizations must develop, implement, monitor, and regularly update a comprehensive information security program."[244] Meanwhile, on the private ordering side, the NIST Framework extensively describes the process for establishing a security program and the ways such a program could integrate the Framework.[245] Similar programmatic commitments are central to other private frameworks, including CISSP certification, PCI standards, vendor contracts, and insurance policies.

The creation of a "comprehensive data security program" has also been an explicit condition in most FTC consent decrees arising from data security cases under consumer protection law.[246] The *LabMD* court implies that this FTC demand is an

242. *Compare* 45 C.F.R. § 164.308 (2016) (administrative safeguards), *with id.* § 164.310 (physical safeguards), *and id.* § 164.312 (technical safeguards).

243. CALIFORNIA REPORT, *supra* note 84, at 27.

244. *Id.* at 29.

245. *See* NIST FRAMEWORK, *supra* note 126, at 13–15.

246. *See, e.g.*, FTC v. Ruby Corp., No. 1:16-CV-02438, at 4 (D.D.C. Dec. 14, 2016), https://www.ftc.gov/system/files/documents/cases/161214ashleymadison order1.pdf; *In re* ASUSTeK Computer, Inc., File No. 142-3156, 2016 WL 4128217, at *12 (F.T.C. July 18, 2016); *In re* Snapchat, Inc., 2015-1 Trade Cas. (CCH) ¶ 17115, at *7 (Dec. 23, 2014); *In re* Fandango, LLC, 2015-1 Trade Cas. (CCH) ¶ 17098, at *6 (Aug. 13, 2014); *In re* Accretive Health, Inc., File No. 122-3077, 2014 WL 726603, at *3 (F.T.C. Feb. 5, 2014).

unprincipled and idiosyncratic departure from the norm.[247] Quite the contrary. While I am continuing to set aside the distinct question of whether the FTC has the power to enforce it, the requirement to have a formal data security compliance program is ubiquitous in both legal and nonlegal frameworks. It certainly is no aberration. Indeed, it has already become part of the duty of data security.

Such programs' focus on human decisionmaking and process is consistent with well recognized aspects of institutional design. It has long been a platitude in IT management that technological safeguards are only one component of data security. The "golden triangle" of "people, process, and technology," borrowed from 1960s organizational theory, has become familiar to those involved in IT strategy.[248] The frameworks' emphasis on the first two of these components lines up with this familiar paradigm.

Attorneys typically are comfortable with this sort of approach. The law habitually advances procedural solutions to address substantive concerns. The Due Process Clauses of the United States Constitution largely guarantee notice and a fair opportunity to make arguments, rather than requiring any particular determinations.[249] The Administrative Procedure Act establishes parameters for federal executive agencies such as notice-and-comment rulemaking and judicial review.[250] Thus it is no surprise that legal rules addressing data security risk also use procedural mechanisms to establish structures that indirectly but effectively reduce risk.

247. *See* LabMD v. F.T.C., 894 F.3d 1221, 1230 (11th Cir. 2018) (mocking the "sweeping prophylactic measures" contemplated by the proposed consent order before the court).

248. It is the sort of truism that can be difficult to trace to its origins. I have seen it credited to a paper by H.J. Leavitt. Harold J. Leavitt & Bernard M. Bass, *Organizational Psychology*, 15 ANN. REV. PSYCHOL. 371, 386–87 (1971). It was popularized in the late 1990s and early 2000s by, among others, the well-known data security expert Bruce Schneier. *See* Bruce Schneier, *People, Process, and Technology*, SCHNEIER ON SECURITY (Jan. 30, 2013, 12:20 PM), https://www.schneier.com/blog/archives/2013/01/people_process.html; Bruce Schneier, *The Process of Security*, SCHNEIER ON SECURITY (Apr. 2000), https://www.schneier.com/essays/archives/2000/04/the_process_of_secur.html; *see also* OFFICE OF GOV'T COMMERCE (UK), ITIL SERVICE OPERATION 165–66 (2007) (illustrating that changes in IT operations may be triggered by technological changes, procedural changes, or personnel changes); *cf.* SHACKELFORD, *supra* note 19, at 226–30 (discussing best practices for "people and processes" in private sector cybersecurity).

249. *See* Mathews v. Eldridge, 424 U.S. 319, 332–35 (1976).

250. *See* 5 U.S.C. §§ 500–706 (2017).

In data security, the development, enforcement, and assessment of a data security policy captures a core aspect of what David Thaw has called "Management-Based Regulatory Delegation."[251] In this model, government authorities mandate that companies develop internal regulations—their "company law"—concerning data security.[252] As Thaw explains, a requirement for companies to generate their own policy retains flexibility. This is necessary for a host of reasons, including the speed with which the technology concerning both threats and protection evolves as well as the differences in risk profiles among businesses.[253] This, again, is a procedural requirement that a policy exist, rather than a substantive rule directly regulating security-oriented behavior. It stems in part from the recognition that the very process of developing a policy drives security improvement—as the business-school aphorism suggests, whatever gets measured gets managed. This "operationalization" of best practices within corporate management, as Kenneth Bamberger and Deirdre Mulligan have found, helps catalyze greater internal attention to privacy (including data security) and engagement with outside stakeholders.[254]

As a whole, the fourteen frameworks make demands concerning at least five separate aspects of these compliance systems, each described in greater detail in this subsection: risk assessment, formal policy, leadership, training, and audit. When deployed in a data custodian's organization, these components are cyclical.

251. Thaw, *supra* note 75, at 293 & n.18.

252. *See* LOTHAR DETERMANN, DETERMANN'S FIELD GUIDE TO DATA PRIVACY LAW: INTERNATIONAL CORPORATE COMPLIANCE (3d ed. 2017) (providing guidance regarding how companies should develop data security practices so that they comply with government regulation).

253. *See* Thaw, *supra* note 75, at 325–26.

254. See BAMBERGER & MULLIGAN, *supra* note 7, at 219–37.

The frameworks expect custodians to begin with risk assessment, as mentioned above.[255] That assessment informs the adoption of a formal written compliance policy. Many frameworks require that data custodians designate specific employees to lead those compliance efforts, and then that other employees receive appropriate training about the policy. Finally, most of the frameworks presume that data custodians test the effectiveness of their compliance architecture. Based on this self-audit, they are to revisit their risk assessment and start the cycle again: revising their policies, leadership approaches, and training accordingly.

Risk Assessment. The duty of data security requires that a plan will be based on a thorough and ongoing assessment of a data custodian's risks, probably in connection with a comprehensive data mapping exercise to determine the flow of information through the organization and the places it may be vulnerable.[256] For example, the CIS Controls designate six of its twenty named controls as most essential, and three of those are an inventory of hardware, an inventory of software, and "continuous vulnerability management."[257] The NIST Framework and FINRA's small

255. *See supra* Part II.A.

256. *See generally* Hardin, *supra* note 241 (presenting data security methodology based in Enterprise Risk Management).

257. CIS CONTROLS, *supra* note 114, at 3, 11.

business self-assessment tool similarly begin with identification of personal data and associated vulnerabilities.[258]

Legal frameworks, like these private ones, also begin with risk. FTC consent decrees have typically mandated a comprehensive review of data security vulnerabilities and responses as part of an initial audit, followed by regularly scheduled follow-up audits to revisit them.[259] In its primary guidance, HHS similarly emphasizes "risk analysis" as a centerpiece of compliance with the HIPAA Security Rule[260]—and the agency has even developed a "Security Risk Assessment Tool" that can be downloaded from popular app stores.[261] The New York regulations include "periodic risk assessments" as a core obligation for covered financial institutions, requiring that the assessments be based on criteria articulated in advance.[262]

Formal Policy. After a risk assessment, the frameworks consistently expect a data custodian to develop its own internal policy or "company law" consistent with the identified threats.[263] The frameworks differ in their degree of specificity about the contents of this policy. For illustration, consider the financially oriented frameworks. The Gramm-Leach-Bliley Act instructs financial regulatory agencies to:

> establish appropriate standards for the financial institutions subject to their jurisdiction relating to administrative, technical, and physical

258. NIST FRAMEWORK, *supra* note 126, at 14–15; FINRA Checklist, *supra* note 180.

259. *In re* Uber Techs., Inc., File No. 152-3054, 2018 WL 1836642, at *2–3 (F.T.C. Apr. 11, 2018); FTC v. Ruby Corp., No. 1:16-CV-02438, at 4–7 (D.D.C. Dec. 14, 2016), https://www.ftc.gov/system/files/documents/cases/161214ashleymadisonorder1.pdf; Dave & Buster's, Inc., 149 F.T.C. 1449, 1455–57 (2010), 2010 WL 9434816, at *4–5.

260. *Summary of the HIPAA Security Rule*, HHS.GOV (July 26, 2013), https://www.hhs.gov/hipaa/for-professionals/security/laws-regulations/index.html ("[R]isk analysis affects the implementation of all of the safeguards contained in the Security Rule. . . . Risk analysis should be an ongoing process, in which a covered entity regularly reviews its records to track access to e-PHI and detect security incidents, periodically evaluates the effectiveness of security measures put in place, and regularly reevaluates potential risks to e-PHI."); *see also Guidance on Risk Analysis*, HHS.GOV (Mar. 9, 2017), https://www.hhs.gov/hipaa/for-professionals/security/guidance/guidance-risk-analysis/index.html.

261. *See Security Risk Assessment*, HEALTHIT.GOV (Nov. 15, 2018), https://www.healthit.gov/topic/privacy-security-and-hipaa/security-risk-assessment.

262. N.Y. COMP. CODES R. & REGS. tit. 23, § 500.09 (2018) ("Each covered entity shall conduct a periodic risk assessment of the covered entity's information systems sufficient to inform the design of the cybersecurity program as required by this Part.").

263. *See* DETERMANN, *supra* note 252.

> safeguards—
>
> (1) to insure the security and confidentiality of customer records and information;
>
> (2) to protect against any anticipated threats or hazards to the security or integrity of such records; and
>
> (3) to protect against unauthorized access to or use of such records or information which could result in substantial harm or inconvenience to any customer.[264]

Some of these agencies, such as the Securities and Exchange Commission (SEC), wrote rules that simply ordered the financial institutions under their purview to develop internal policies that did those three things, repeating the statutory language verbatim.[265] The FTC went further in its version, not only repeating the congressional statement of goals for an information security program, but also listing the elements that each program should contain.[266] That said, the authorities also communicate their expectations through methods other than formal rules. For example, the SEC has undertaken enforcement actions and issued less formal guidance for regulated firms.[267] In addition, FINRA's role as a licensing authority makes it another source of supervision, and FINRA issues extensive technical assistance to help broker-dealers meet their duty of data security.[268]

The illustrative range of specificity from the financial sector is reflected throughout the frameworks. The target profiles under the NIST Framework, the comprehensive security policy mandated in FTC consent orders, and the policies required under New York's regulations all embody this same principle of risk-guided internal security policies created by data custodians.

Leadership. There has been some consternation among U.S. privacy lawyers and their clients about a requirement that took effect in 2018 under the European Union's new data protection regime, mandating that every company processing data in the EU name a "data protection officer."[269] Few of them seem to have noticed how much the American system has already begun

264. 15 U.S.C. § 6801(b)(1)–(3) (2017).

265. *See* 17 C.F.R. § 248.30 (2018).

266. *See* 16 C.F.R. § 314.4 (2018).

267. *See, e.g.*, *Cybersecurity, the SEC and You*, U.S. SEC. & EXCHANGE COMMISSION (Aug. 21, 2018), https://www.sec.gov/spotlight/cybersecurity.

268. *See Cybersecurity: Guidance*, FINRA—FIN. INDUSTRY REG. AUTHORITY, http://www.finra.org/industry/cybersecurity (last visited Nov. 20, 2018) (providing guidance on various data security issues).

269. General Data Protection Regulation, *supra* note 82, at art. 37.

to require similar formal leadership designations, at least for the data security components of privacy compliance.

The New York regulations go particularly far, requiring data custodians to name a CISO—either an employee or an outside provider—who must write an annual report to the board of directors covering topics specified in the rules.[270] But other frameworks also envision high-ranking executives focused intently on the development of a data security compliance program. The insurance underwriting documents reviewed earlier, for example, typically expect that senior corporate officials are directly responsible for the management of data security.[271]

The drive toward named security leadership is in keeping with the systems-oriented approach of U.S. data security law. What better symbolizes the institutional importance of data security than embedding it in the organizational chart? Of course, just naming an official does not itself provide that person the tools to succeed.[272] At times, these specialized managers can become public relations scapegoats; Equifax, for example, loudly fired its security executives immediately after its breach became public.[273] But hopefully CISOs and similar executives also have the capacity to build bridges between bureaucratic islands involved in data security such as legal departments, IT managers, and developers of new products.[274] And at the highest levels of an institution, their singular commitment to security may make

270. N.Y. COMP. CODES R. & REGS. tit. 23, § 500.04 (2018) ("Each Covered Entity shall designate a qualified individual responsible for overseeing and implementing the Covered Entity's cybersecurity program and enforcing its cybersecurity policy . . . .").

271. *See Sample Cyberinsurance Applications*, *supra* note 208.

272. *See* Justin Dolly, *The Rise of the CISO*, CIO REV., https://security.cioreview.com/cioviewpoint/the-rise-of-the-ciso-nid-23914-cid-21.html (last visited Nov. 20, 2018). The author cites poll data finding that "only seventy percent of CISOs said they strongly agree that they are receiving the organizational support they need to do their jobs effectively." *Id.* I would suggest instead that it is a shockingly positive finding if more than two-thirds of executives responsible for any function in any modern American corporation say they already have the resources and support they need.

273. *See* Jennifer Surane, *Equifax Says CIO, Chief Security Officer to Exit After Hack*, BLOOMBERG NEWS (Sept. 15, 2017), https://www.bloomberg.com/news/articles/2017-09-15/equifax-says-cio-chief-security-officer-to-leave-after-breach.

274. *See* SHACKELFORD, *supra* note 19, at 226–27 (describing the interaction between CISOs and other departments within an organization).

them strong advocates for its importance and help data security compete for resources against other organizational priorities.[275]

Training. The strongest policy and the most committed management will mean nothing if rank-and-file employees disregard a data custodian's duty of data security.[276] Attackers exploit knowledge gaps by tailoring phishing attacks and other techniques that can trick personnel who do not have strong data security awareness.[277] Most of the frameworks expect data custodians to train employees throughout the organization to ensure that they adhere to policy. The HIPAA Security Rule, for example, states that a covered entity must train "all members of its workforce (including management)."[278] The same is true for frameworks created more organically out of industry practice, such as the NIST Framework or FINRA rules.[279] And here, again, insurers require details of policyholders' training programs as preconditions for coverage.[280]

Audit. Finally, systematic requirements come full circle when initial assessments must be revisited in light of actual performance and evolving threats. The findings contribute to better understanding of risk and to improvements in policy and training. Numerous frameworks call for continual risk assessment.[281]

275. BAMBERGER & MULLIGAN, *supra* note 7, at 177–80 (providing examples of the benefits of the "managerialization" of privacy).

276. *See* SHACKELFORD, *supra* note 19, at 227–28 ("Although leadership and high-level coordination are imperative, cybersecurity is also the responsibility of every employee. Thus, it is vital that firms help educate and assess employees' cybersecurity habits . . . ."); PETER P. SWIRE & KENESA AHMAD, FOUNDATIONS OF INFORMATION PRIVACY AND DATA PROTECTION 104–11 (2012) (discussing employee negligence as a common cause of data breaches and the importance of training employees on security issues).

277. *See* CIS CONTROLS, *supra* note 114, at 43–45 (discussing how hackers exploit lack of employee awareness as a security vulnerability and calling for assessments of employee knowledge and training to fill gaps).

278. 45 C.F.R. § 164.308(a)(5)(i) (2016).

279. FINRA REPORT, *supra* note 19, at 31 ("[C]ybersecurity training is an essential component of any cybersecurity program. Even the best technical controls on a firm's systems can be rapidly undermined by employees who are inattentive to cybersecurity risks."); NIST FRAMEWORK, *supra* note 126, at 24–25.

280. *See, e.g.*, *Sample Cyberinsurance Applications*, *supra* note 208.

281. *See, e.g.*, 45 C.F.R. § 164.308(a)(8) (prescribing periodic assessments under HIPAA); CIS CONTROLS, *supra* note 114, at 11–12 (describing the CIS framework's "Continuous Vulnerability Management" step); START WITH SECURITY, *supra* note 72, at 12 (describing the "ongoing process" of security under the FTC framework); NIST FRAMEWORK, *supra* note 126, at 4 (describing the "recurring risk assessments" supported by the NIST Framework); STEWART, *supra* note 193, at 74 (describing the continual risk assessment of CISSP).

This effectively becomes a duty of ongoing monitoring. Some frameworks have begun specifying that data custodians have a duty to test their security systems, sometimes by particular means. These might be simpler scans and penetration tests or they might entail full "red team" simulations.[282] The PCI DSS explicitly requires penetration testing as part of the design of new systems and on a set schedule thereafter.[283] The New York regulations require either continuous monitoring or, at a minimum, annual penetration testing and biannual vulnerability assessments.[284] The FTC has taken action against over a dozen companies for failure to test against widely known vulnerabilities.[285] This firmly established requirement of consistent self-examination helps security systems remain up-to-date with technology and changing threat models. Naturally, such backward-looking reviews are constrained by architectural choices that have already been made, but they also present new opportunities to think broadly and perceive vulnerabilities that might not have been evident before.[286]

In summary, the fourteen frameworks agree overwhelmingly on the necessity of a formal data security program and on its key components. The duty of data security that emerges from this consensus requires that data custodians engage in a cyclical process with mechanisms to assess risk, develop appropriate policy, appoint leaders and train other employees, and continuously audit and improve procedures.

C. ARCHITECTURAL REQUIREMENTS

For the most part, the fourteen frameworks do not demand specific implementations to protect data security. They have a good deal more to say about the programmatic structures discussed in the previous Section than about the technological structures that actually house personal data and keep it safe.[287]

282. *See* Doug Drinkwater & Kacy Zurkus, *Red Team Versus Blue Team: How to Run an Effective Simulation*, CSO (July 26, 2017), https://www.csoonline.com/article/2122440/disaster-recovery/emergency-preparedness-red-team-versus-blue-team-how-to-run-an-effective-simulation.html.

283. PCI DSS, *supra* note 169, at 100–02.

284. N.Y. COMP. CODES R. & REGS. tit. 23, § 500.05 (2018).

285. START WITH SECURITY, *supra* note 72, at 10.

286. *See* STEVEN M. BELLOVIN, THINKING SECURITY: STOPPING NEXT YEAR'S HACKERS 225–28 (2016).

287. *See supra* notes 44–47 and accompanying text (comparing the HIPAA Security Rule's significant emphasis on administrative safeguards with a smaller amount of discussion directed to technical and physical safeguards).

The frameworks generally assume that the correct procedures will yield the correct technical solutions.

More fundamentally, however, the frameworks recognize the futility of providing cookbook recipes in these circumstances. Data security is highly dynamic in two dimensions. First, as described in Section A, different data custodians have dramatically different, and often-changing, levels of risk and resources.[288] Second, the specific technology of both attacks and defenses evolves constantly.[289] Safeguards that used to work may not be effective tomorrow, and previously unknown threats emerge regularly.

In this environment, the frameworks typically provide broad design principles that may be implemented through a wide variety of technological means, provided they are within the range of reasonableness. Over time, however, certain of these principles have become canonical, so that they have been incorporated widely in both the legal and private frameworks presented in Part I. In a few cases, particular fundamental technical responses are widely regarded as necessities. Increasingly, a failure to design architecture consistently with these most commonly accepted principles represents a breach of the duty of data security. This Section identifies a few of these requirements.

Access Controls. The most basic components of security architecture limit access to potentially vulnerable data. A fundamental tenet of many security methodologies, including the CISSP, centers on the "principle of least privilege"—a role-based authorization model that allows employees access only to information necessary for their job functions.[290] Many frameworks also call for appropriate network design features to prevent both insiders and outsiders from bypassing access controls, such as

288. *See supra* notes 240–41 and accompanying and subsequent text (discussing how the reasonableness of precautions varies with the custodian).

289. *See* Ronald N. Weikers, *Security and Privacy in the Networked World*, *in* 1 DATA SECURITY AND PRIVACY LAW, *supra* note 241, at 130–31 (discussing the rate of increase in new data security threats).

290. STEWART, *supra* note 193, at 662–68; *see also* FINRA REPORT, *supra* note 19, at 17–20 (providing detailed instructions for the design of an identity and access management structure, while also making it clear that there should be risk-based flexibility in its implementation).

the continual maintenance of firewalls,[291] audits to monitor access and detect unauthorized use,[292] or limitations on administrative privileges.[293] Finally, reasonable data security also encompasses physical security, including limited facility access, timed lockouts at workstations, clear rules about the use of laptops and other portable storage, and safe storage of servers and backup media.[294] When frameworks spell out these exemplary access control mechanisms, typically they leave individual data custodians free to select the precise combination of safeguards they use—consistent with reasonable risk assessment, naturally.

Encryption. The duty of data security basically mandates encryption in certain circumstances. FINRA calls encryption "a critically important effective practice in a firm's cybersecurity control arsenal."[295] Technical standards such as the CIS Controls and the PCI DSS provide detailed guidance concerning the best practices for using encryption.[296] The safe harbor for encrypted data in state breach notification statutes further ensconces encryption as an aspect of the duty of data security by creating strong additional incentives to encrypt data—namely, avoiding notice obligations in the event of an incident.[297]

Encryption mandates usually correlate with heightened risk. Some frameworks, for example, recommend only that par-

291. *See* CIS CONTROLS, *supra* note 114, at 27–29; *supra* note 176 and accompanying text (describing details of firewall requirements in PCI DSS).

292. *See, e.g.*, CIS CONTROLS, *supra* note 114, at 19; START WITH SECURITY, *supra* note 72, at 8; NIST FRAMEWORK, *supra* note 126, at 29.

293. *See, e.g.*, START WITH SECURITY, *supra* note 72, at 4 (discussing FTC action against Twitter for failure to control employee access to administrative credentials); *supra* notes 157–59 and accompanying text (describing detailed requirements in the CIS Controls concerning administrative privileges).

294. *See, e.g.*, 45 C.F.R. § 164.310 (2016) (establishing requirements in the HIPAA Security Rule for physical safeguards including access to the facility and access to computer workstations); START WITH SECURITY, *supra* note 72, at 13 (recommending procedures for securing devices and paper files); NIST FRAMEWORK, *supra* note 126, at 34 ("Policy and regulations regarding the physical operating environment for organizational assets are met."); STEWART, *supra* note 193, at 385–416 (reviewing numerous physical security considerations).

295. FINRA REPORT, *supra* note 19, at 20.

296. *See* CIS CONTROLS, *supra* note 114, at 32–33 (recommending encryption for data protection in multiple scenarios); PCI DSS, *supra* note 169, at 47 (requiring strong cryptography when transmitting sensitive cardholder data over public networks).

297. *See supra* note 89 and accompanying text (citing and quoting encryption incentives in state breach notification statutes).

ticularly sensitive data such as health information should be encrypted.[298] Many encourage encryption of data at points of particular vulnerability: when exposed "in transit," when stored on portable devices such as laptops or thumb drives, and possibly when in cloud-based storage.[299] The Massachusetts regulations mandate encryption in all these situations.[300]

These encryption requirements are fairly flexible, however. The HIPAA Security Rule, for example, requires encryption of data in transit, but only "whenever deemed appropriate."[301] And notably, none of the frameworks mandates a single technical specification for acceptable encryption, instead leaving that more precise determination open-ended. This is important, because encryption is not a security panacea and there are costs as well as benefits to its deployment.[302] Thus, even the PCI DSS, often among the most technically specific of the frameworks,[303] allows numerous alternative implementations in its "Point-to-Point Encryption (P2PE)" requirements.[304]

Multifactor Authentication. One of the newest specific architectural controls found in the frameworks is the use of multifactor authentication to augment or replace simpler and less effective access methods such as passwords.[305] Multifactor authentication relies on a combination of methods for an individual to establish identity, so that even if an attacker compromises one

298. *See, e.g.*, 45 C.F.R. § 164.312(a)(2)(iv) (requiring encryption procedures for protected health information under the HIPAA Security Rule); START WITH SECURITY, *supra* note 72, at 6 (recommending "strong cryptography" for "sensitive personal information"); CALIFORNIA REPORT, *supra* note 84, at 36–37 (emphasizing that the use of encryption is especially important in the health care sector).

299. *See, e.g.*, 45 C.F.R. § 164.312(e)(1) (requiring stricter technical safeguards under the HIPAA Security Rule for "[t]ransmission security"). The sample insurance forms examined earlier all ask about encryption, distinguishing between data at rest and in transit. *See Sample Cyberinsurance Applications*, *supra* note 208.

300. 201 MASS. CODE REGS. 17.04(3), (5) (2017).

301. 45 C.F.R. § 164.312(e)(2)(ii).

302. *See* BELLOVIN, *supra* note 286, at 105–06 (discussing the disadvantages of encryption).

303. *See supra* notes 169–77 and accompanying text (describing the requirements of the PCI DSS framework).

304. *PCI Point-to-Point Encryption (P2PE)™ Solutions*, PCI SECURITY STANDARDS COUNCIL, https://www.pcisecuritystandards.org/assessors_and_solutions/point_to_point_encryption_solutions (last visited Nov. 20, 2018).

305. *See* STEWART, *supra* note 193, at 564 (listing numerous flaws that make passwords "weak security mechanisms").

method, access to data will still be blocked.[306] Common examples of multifactor authentication include mixing "something you know" (such as a password) with "something you have" (such as a smartcard, a biometric identifier, or a unique code sent to the owner's mobile device).[307] We see examples of multifactor authentication in daily life such as "chip and PIN" debit cards[308] and Google's account recovery system.[309] Even *Teen Vogue*—which has been remarkably enterprising and well-informed concerning issues of digital policy—published an article extolling multifactor authentication and urging readers to activate it in their social media accounts.[310]

The New York regulations made waves by legally requiring the adoption of multifactor authentication "for any individual accessing the Covered Entity's internal networks from an external network."[311] Even in this framework, however, the specific mandate is only a presumption; a CISO may approve "the use of reasonably equivalent or more secure access controls."[312]

Rather than a mandate, most other frameworks now suggest that data custodians should consider multifactor authentication, at least in situations involving external network access, sensitive data, or both. A 2018 revision of the NIST Framework added an entirely new subcategory to the framework requiring authentication "commensurate with the risk of the transaction."[313] The Chubb/Ace insurance application asks whether the applicant "use[s] multi-factor authentication for remote network

306. *See* N.Y. COMP. CODES R. & REGS. tit. 23, § 500.01(f) (2018) (defining multifactor authentication).

307. *See* STEWART, *supra* note 193, at 566–73 (describing different methods for multifactor authentication).

308. *See* Dave Roos, *How Chip and PIN Credit Cards Work*, HOW STUFF WORKS (May 16, 2014), https://money.howstuffworks.com/personal-finance/debt-management/chip-and-pin-credit-cards.htm.

309. *See Tips to Complete Account Recovery Steps*, GOOGLE ACCT. HELP, https://support.google.com/accounts/answer/7299973?hl=en (last visited Nov. 20, 2018).

310. Nicole Kobie, *Why Two-Factor Authentication Is So Important*, TEEN VOGUE (Mar. 27, 2017), https://www.teenvogue.com/story/why-two-factor-authentication-is-important.

311. N.Y. COMP. CODES R. & REGS. tit. 23, § 500.12(b).

312. *Id.*

313. NIST FRAMEWORK, *supra* note 126, at 30.

access originating from outside the company network by employees and third parties (e.g., VPN, remote desktop)."[314] The California Attorney General's report stated that all companies "should" use multifactor authentication for access to "critical systems and sensitive data, such as medical information, financial information, [and] Social Security numbers," and also recommended that firms should make it available to users of "consumer-facing online accounts that contain sensitive personal information. Such accounts include online shopping accounts, health care web sites and patient portals, and web-based email accounts."[315] The FTC has more gently suggested that all data custodians evaluate multifactor authentication.[316]

Once again, the precise method of deploying multifactor authentication is left up to individual data custodians, and there are few absolute requirements to use it. But as passwords become increasingly poor security measures, reasonableness analysis itself will begin to require major shifts toward newer access control methods such as multifactor authentication.[317]

D. WORST PRACTICES

In addition to insisting upon certain procedural structures and a few particular architectural safeguards, some of the frameworks also tell data custodians exactly what they should *not* do. Instead of recommended best practices, I call these "worst practices"—the types of mistakes that are serious and difficult to excuse. For the most part, these worst practices are already dramatic departures from the requirements of the duty of data security outlined in the first three Sections of this Part. They are

314. ACE PRIVACY PROT., CYBER AND PRIVACY INSURANCE APPLICATION FORM 4 (2015).

315. CALIFORNIA REPORT, *supra* note 84, at 35–36.

316. START WITH SECURITY, *supra* note 72, at 5.

317. *See* BELLOVIN, *supra* note 286, at 108–14 (describing the weaknesses of passwords as a security measure); Taylor Armerding, *Killing the Password: FIDO Says Long Journey Will Be Worth It*, CSO (July 12, 2016), https://www.csoonline.com/article/3092844/security/killing-the-password-fido-says-long-journey-will-be-worth-it.html (describing industry efforts to "kill the password" by adopting newer authentication methods, and noting, "[t]here is little debate among security experts that passwords are a lousy, obsolete form of authentication"); *see also History of FIDO Alliance*, FIDO ALLIANCE, https://fidoalliance.org/about/history (last visited Nov. 20, 2018) (describing development of an industry coalition to "advance the vision of device based, simple secure authentication designed to eliminate the reliance on passwords").

not reasonable, they should have been prevented by a robust policy backed by risk assessment and training, and they do not represent sound network design. So, they contravene the duty of data security already—but frameworks often single out worst practices as especially egregious examples of violations.

There are plenty of worst practices specified in various frameworks. Equifax's reported failure to install a widely distributed update to patch a known security flaw in an Adobe enterprise system will qualify as a worst practice.[318] Enforcement actions by regulators who supervise the frameworks provide many other such cautionary tales. In the *Wyndham* case, for example, the FTC presented many allegations of atrocious data security practices by the defendant, including the use of out-of-the-box default passwords for servers Wyndham connected to a network, the storage of payment card data in plain text format, and a lack of firewalls and other elementary access controls.[319] Likewise, the SEC's first enforcement action under the Safeguards Rule involved a financial firm accused of storing unencrypted personal data about approximately 100,000 individuals on a third-party server without imposing any security requirements on the vendor.[320] HHS collected a $2.7 million penalty from a university hospital system for failing to respond adequately after repeated thefts of laptops and thumb drives containing unencrypted protected health information.[321]

Worst practices are simply analogues to better ones. But they also provide a more specific list of examples to guide the development of data security policy and deployment. They are the opposite of an expectation of perfection. All of the frame-

318. *See supra* notes 1–2 and accompanying text (discussing alleged causes of Equifax breach).

319. FTC v. Wyndham Worldwide Corp., 799 F.3d 236, 240–42 (3d Cir. 2015) (describing these and other FTC allegations about Wyndham's practices).

320. R.T. Jones Capital Equities Mgmt., Inc., Investment Advisers Act of 1940 Release No. 4204, 112 SEC Docket 2848 (Sept. 22, 2015), 2015 WL 5560846, at *1–2.

321. *Widespread HIPAA Vulnerabilities Result in $2.7 Million Settlement with Oregon Health & Science University*, HHS.GOV (July 18, 2016), http://wayback.archive-it.org/3926/20170127185938/https://www.hhs.gov/about/news/2016/07/18/widespread-hipaa-vulnerabilities-result-in-settlement-with-oregon-health-science-university.html; *see also* OFFICE FOR CIVIL RIGHTS, U.S. DEP'T OF HEALTH & HUMAN SERVS., RESOLUTION AGREEMENT AND CORRECTIVE ACTION PLAN BETWEEN OCR AND OREGON HEALTH & SCIENCE UNIVERSITY 1–2, https://www.hhs.gov/sites/default/files/ohsuracap_508.pdf (last visited Nov. 20, 2018).

works say they scale to the appropriate size based on risk calculations. Several explicitly contemplate different levels of maturity—such as the NIST Framework with its inclusion of target profiles as organizational goals.[322] But critics who crave more concrete guidance can take comfort in the existence of a sizable list of "don'ts" to help them understand what *not* to do. These blunders go down in the law books as worst practices to be avoided by all data custodians.

III. ASSESSING THE DUTY OF DATA SECURITY

So far, this Article has analyzed fourteen representative frameworks that govern the duty of data security and has shown substantial overlap between them. This Part explains why the present arrangement is both familiar and desirable. The law is coming to recognize a duty of data security. Rather than a simple checklist, it is a principles-based duty, embodied in flexible standards. Its content is derived predominantly from the private ordering and emerging practices of responsible data custodians themselves and the IT professionals who advise them. Finally, its demands are calibrated to the capacity of data custodians and the risks they face based on their scale, their vulnerabilities, and the nature of the personal data they hold. This Part considers all these attributes of the duty of data security.

A. ROOTED IN FLEXIBLE STANDARDS

The reasonableness standards found throughout the fourteen frameworks make some people uncomfortable. Many data custodians are seeking absolute certainty that the steps they are taking suffice under the law. I have similar conversations with my very intelligent first-year law students every September, when elliptical Supreme Court precedents leave them begging for the "right answer" or the "bottom line." Most IT professionals were trained in computer science, a discipline in which most things that matter can be expressed in the ones and zeroes of binary code. Their frustration, like that of new law students, is understandable. They crave rules, and the law gives them standards.

Unfortunately, in my experience, many technologists and attorneys fail to communicate effectively across the divide caused by their methodological differences. It is an old problem.

322. *See supra* notes 144–47 and accompanying text (describing the NIST Framework's risk profiles and mechanisms for continuous improvement).

The British author and scientist C.P. Snow warned in his famous 1959 lecture, "The Two Cultures," that "literary intellectuals" and "physical scientists" were separated by "a gulf of mutual incomprehension—sometimes (particularly among the young) hostility and dislike, but most of all lack of understanding."[323] Lawyers are not literary intellectuals, nor are IT professionals physical scientists, but each group is closer to a different pole than the other, and the intercultural incomprehension described by Lord Snow affects them both.

It might help if we attorneys reassured our technical colleagues more directly that broad reasonableness standards are among the oldest cornerstones of law. The examples are legion. Perhaps the most prominent reasonableness standard in law is the general measure of liability for negligence torts—from car crashes to medical malpractice to slip-and-falls on unshoveled sidewalks. In tort law, the reasonable person is one who "exercise[es] those qualities of attention, knowledge, intelligence, and judgment which society requires of its members for the protection of their own interests and the interests of others."[324] This is the very same standard upon which many civil suits seeking to hold data custodians responsible for security breaches would proceed, if they ever reached judgment.[325]

Reasonableness standards also permeate other aspects of privacy law, not just the duty of data security. Under a well-established Fourth Amendment test, for example, law enforcement must respect an individual's "*reasonable* expectations of privacy" when engaging in a search or seizure without a warrant.[326] And data custodians who want to protect a trade secret in addition to personal information must demonstrate that they made "efforts that are reasonable under the circumstances to maintain its secrecy" or risk losing its legal protection.[327]

323. C.P. Snow, *The Rede Lecture, in* THE TWO CULTURES 4 (1998); *see also* Peter Lee, *Patent Law and the Two Cultures*, 120 YALE L.J. 2, 4–5 (2010) (discussing Lord Snow's lecture).

324. RESTATEMENT (SECOND) OF TORTS § 283, cmt. b (AM. LAW INST. 1965).

325. *See supra* notes 27–33 and accompanying text (providing examples of tort theories in data breach cases and barriers to achieving final judgment in such cases).

326. *See* United States v. Jones, 565 U.S. 400, 405–06 (2012) (discussing the importance of the test); *id.* at 419 (Alito, J., concurring) (arguing the test should be applied in all cases); Katz v. United States, 389 U.S. 347, 360–61 (1967) (Harlan, J., concurring) (establishing the test).

327. *See* UNIF. TRADE SECRETS ACT § 1(4)(ii) (UNIF. LAW COMM'N 1985); LOUIS ALTMAN & MALLA POLLACK, 3 CALLMANN ON UNFAIR COMPETITION,

Most lawyers also understand the relative advantages of rules and standards, thanks to longstanding debate about them in legal literature.[328] There are two ways to understand the distinction between rules and standards. One difference is that rules stipulate brighter lines while standards rely on more general criteria.[329] Under another widely accepted account, rules already contain their principal substance before the occurrence of whatever activity they regulate, while adjudicators supply content to standards only after the fact.[330] A speed limit is a rule in both senses: the appropriate speed is precisely articulated as a number, which is announced in advance. A requirement to drive at "reasonable speed" would be a standard: defined with room for discretion, which would only be applied afterward. By either of these meanings, the duty of data security expressed in the fourteen frameworks is a standard. Its reasonableness requirement does not instruct data custodians about exactly what they should do, and the adequacy of their security precautions typically will

TRADEMARKS & MONOPOLIES § 14:26 (4th ed. 2018) ("Reasonable efforts at secrecy are required . . . .").

328. *See, e.g.*, Isaac Ehrlich & Richard A. Posner, *An Economic Analysis of Legal Rulemaking*, 3 J. LEGAL STUD. 257, 272 (1974) (discussing the importance of cost considerations when choosing between rules and standards in lawmaking); Russell B. Korobkin, *Behavioral Analysis and Legal Form: Rules vs. Standards Revisited*, 79 OR. L. REV. 23, 43–45 (2000) (explaining the use of bounded rationality, preference endogeneity, and norm compliance in the analysis of rules and standards); Mark S. Popofsky, *Defining Exclusionary Conduct: Section 2, The Rule of Reason, and the Unifying Principle Underlying Antitrust Rules*, 73 ANTITRUST L.J. 435, 448–49 (2006) (discussing the effects of "error costs" and "legal process costs" on conduct and their relationship to the use of rules and standards).

329. *See, e.g.*,David Franklin, *The Roberts Court, the 2008 Election & the Future of the Judiciary*, 6 DEPAUL BUS. & COM. L.J. 513, 515 (2008) (discussing the preference of Chief Justice Roberts for "bright-line" rules); Louis Kaplow, *General Characteristics of Rules*, *in* 5 ENCYCLOPEDIA OF LAW & ECONOMICS 502, 502 (Boudewijn Bouckaert & Gerrit De Geest eds., 2000) ("The most commonly noted characteristic of rules concerns the degree of precision, detail, or complexity they embody: how finely are different sorts of behavior to be distinguished?"); Larry Alexander, *Incomplete Theorizing: A Review Essay of Cass R. Sunstein's Legal Reasoning and Political Conflict*, 72 NOTRE DAME L. REV. 531, 541 (1997) (book review) ("Rules are often described as 'bright-line' . . . .").

330. *See* Louis Kaplow, *Rules Versus Standards: An Economic Analysis*, 42 DUKE L.J. 557, 568–70 (1992) (illustrating the process by which the government judges conduct ex ante and applies a standard); Eric Posner, *Standards, Rules, and Social Norms*, 21 HARV. J.L. & PUB. POL'Y 101, 101–03 (1997) (describing the legislative enactments of a standard as a delegation of authority to the judiciary to evaluate the action); Cass R. Sunstein, *Problems with Rules*, 83 CALIF. L. REV. 953, 961–62 (1995) (arguing the rules specify outcomes before a court reaches its decision).

be judged after a breach, or at least after a data custodian's security measures have been put in place.

To speak the language of our technical colleagues for a moment: the reliance of data security law on standards over rules is a feature rather than a bug. The primary advantage is flexibility, and data security requirements must be flexible.

Perhaps the most important and most obvious reason data security rules require flexibility is the inevitability of rapid technological change. Both threats and solutions evolve too quickly to keep precise rules up to date.[331] Broader standards provide guidance to be applied in a dynamic and perhaps unexpected situation. But they also do not let data custodians off the hook. A classic scholarly article about negligence from 1951 explains that, "[a]s scientific knowledge advances, more risks can be discovered and avoided. Those who deal with matters affected by these advances must keep reasonably abreast of them."[332] CISOs and similar data security professionals must constantly update their approaches, and the cyclical risk-based programmatic approach demanded by the duty of data security forces them to do so.[333]

A second problem with relying on rules is the unpredictability inherent in measuring data security harm. Consider a modern regulatory command expressed as a rule rather than a standard: air pollution limits established by the Environmental Protection Agency (EPA)[334] under the authority of the Clean Air Act.[335] These regulations set an acceptable numerical level for each individual pollutant.[336] The threshold for carbon monoxide, for example, is set at "35 parts per million (40 milligrams per

331. Vivek Wadhwa, *Laws and Ethics Can't Keep Pace with Technology*, MIT TECH. REV. (Apr. 15, 2014), https://www.technologyreview.com/s/526401/laws-and-ethics-cant-keep-pace-with-technology (explaining the burdens rapid technological development places on law).

332. Fleming James Jr., *The Qualities of the Reasonable Man in Negligence Cases*, 16 MO. L. REV. 1, 13 (1951) (describing reasonable duties owed by those with specialized knowledge).

333. *Why a Risk-Based Approach Leads to Effective Cybersecurity*, BIZTECH (Dec. 20, 2017), https://biztechmagazine.com/article/2017/12/why-risk-based-approach-leads-effective-cybersecurity (explaining the advantages of the cyclical risk-based approach to data security).

334. *See* National Primary and Secondary Ambient Air Quality Standards, 40 C.F.R. pt. 50 (2017). Notwithstanding the title, these are rules in the classic sense described in text, not standards.

335. *See* Clean Air Act, 42 U.S.C. §§ 7401–31 (2017).

336. *See NAAQS Table*, U.S. ENVTL. PROTECTION AGENCY, https://www.epa.gov/criteria-air-pollutants/naaqs-table (last updated Dec. 20, 2016).

cubic meter) for a 1-hour average concentration not to be exceeded more than once per year."[337] A rule like this simply could not be articulated in data security. The EPA is able to do so in part because it can consult extensive scientific evidence about the quantity of carbon monoxide that is detrimental to human health.[338] The regulations are not static; the Clean Air Act requires the EPA to revisit the determination periodically through an elaborate expert consultation process in order to keep pace with new research.[339] But even when revised, the result is a rule, just like a speed limit: a clear-cut requirement, determined ex ante.

Now compare carbon monoxide pollution to data security vulnerability. While there is broad scientific consensus about the carcinogenic character of carbon monoxide, there is no agreement among policymakers or experts about the dangers associated with data security—not even the nature of the personal harms suffered by those whose information is exposed in breaches.[340] Data security lacks the same types of impartial or scientific metrics available to determine the safe degree of risk.[341] We have seen the effect of this lack of data quite clearly in the challenges facing underwriting for cybersecurity insurance.[342] Data security problems are novel, fast-evolving, and intertwined with numerous human factors. We cannot rely on a scientifically derived target for inclusion in an ex ante rule.

Those who seem to crave a rule for data security instead of a standard should be careful what they wish for. A rule would be a straitjacket, inflexibly demanding precautions that may not respond effectively to the threat or properly measure the dangers. A more open-ended standard is both necessary and desirable.

337. 40 C.F.R. § 50.8(a)(2) (2018).

338. For a list of scientific evidence the EPA consults, see *Reviewing National Ambient Air Quality Standards (NAAQS): Carbon Monoxide (CO) Air Quality Standards*, U.S. ENVTL. PROTECTION AGENCY, https://www.epa.gov/naaqs/carbon-monoxide-co-air-quality-standards (last updated Jan. 18, 2017).

339. *See* 42 U.S.C. §§ 7408–09 (describing the expert consultation process).

340. *See* Solove & Citron, *supra* note 11, at 756–74 (proposing that risk and anxiety suffered by data breach victims should be recognized by courts as compensable harms).

341. *See* Jeff Hughes & George Cybenko, *Quantitative Metric and Risk Assessment: The Three Tenants Model of Cybersecurity*, TECH. INNOVATION MGMT. REV., Aug. 2013, at 15 (offering a new risk assessment model in light of current data's inability to predict future cybersecurity threats).

342. *See supra* note 206 and accompanying text.

B. ADAPTED FROM INDUSTRY PRACTICES

Traditional common law has borrowed from industry practices for a millennium. One of the earliest forms of commercial law, the *lex mercatoria*, originated in the eleventh and twelfth centuries directly from customs and norms among merchants engaged in international trade; it applied to all their interactions with one another in seaports, fairs, and markets.[343] In his magisterial eighteenth century legal treatise, William Blackstone explained the deference to custom under *lex mercatoria* as having "the utmost validity in all commercial transactions; for it is a maxim of law, that '*cuilibet in sua arte credendum est*'"[344]—in English, experts are to be believed concerning their own art. This adoption of commercial practice as the source of legal obligation was such a natural aspect of the common law that Justice Story considered himself to be stating the obvious when he explained, in his 1842 opinion in *Swift v. Tyson*, the eternal and unassailable nature of general commercial law divined from custom rather than from legislation.[345]

The more modern development of the duty of care through common law tort and contract principles extensively consulted industry custom. Contemporary negligence actions have come to presume that "generally recognized and accepted practices in a profession" are part of the duty of care for those engaging in that profession.[346] That duty also incorporates the specialized learning, skills, and experience associated with engagement in an occupation.[347] Courts have imposed this sort of professional duty on doctors and dentists, lawyers and accountants, airplane pilots and plumbers.[348] In the same way, contract doctrine looks to

343. *See* Harold J. Berman & Colin Kaufman, *The Law of International Commercial Transactions (*Lex Mercatoria), 19 HARV. INT'L L.J. 221, 224–28 (1978) (tracing history of the *lex mercatoria*). *See generally* Joel R. Reidenberg, *Lex Informatica: The Formulation of Information Policy Rules Through Technology*, 76 TEX. L. REV. 553 (1998) (comparing *lex mercatoria* to the development of early internet governance through custom and technological design).

344. 1 WILLIAM BLACKSTONE, COMMENTARIES *75.

345. 41 U.S. (16 Pet.) 1, 18 (1842) ("It is observable, that the Courts of New York do not found their decisions upon this point, upon any local statute, or positive, fixed, or ancient local usage: but they deduce the doctrine from the general principles of commercial law.").

346. 65 PAUL M. COLTOFF ET AL., CORPUS JURIS SECUNDUM NEGLIGENCE § 163 (2018).

347. *See* RESTATEMENT (SECOND) OF TORTS § 299A (AM. LAW INST. 1965); *id.* cmt. a.

348. *See id.* cmt. b.

common trade usage to guide interpretation of any ambiguous terms, thus presuming that those within an industry intended their agreement to be typical of the industry's practices.[349] This only occurs when the assumption is reasonable[350]—there's that word again—and sufficiently widespread.[351]

Absorbing professional norms into legal expectations reflects an assumption—shared by principles as disparate as market demand in economics or majority rule in politics—that common behavior and choices are likely to be socially desirable ones.[352] Tort law's recognition of specialized professional rules of conduct can also protect those accused of violating a duty. As one classic article explained, "[t]hose not in the know are prone to set impractical standards when they judge conduct that has caused injury. Evidence that the defendant has followed the ways of his calling checks hasty acceptance of suggestions for unfeasible change."[353] A duty of data security consistent with widespread custom accommodates a moral intuition against penalizing those who behave in the same way as their peers.[354]

With the rise of the administrative state, a much larger proportion of the law has migrated to statutory and regulatory structures, and away from the more amorphous and fact-specific workings of common law adjudication.[355] If anything, however, the adoption of industry standards and practices by legal rulemakers has increased. In the nineteenth century, as Congress tried to govern a rapidly expanding country in an age of slower communication and travel, it often adopted statutes that deferred to local custom in key respects. To take but one example,

349. *See* U.C.C. § 1-205(2) (AM. LAW INST. & UNIF. LAW COMM'N 2017).

350. *See* 12 WILLISTON ON CONTRACTS § 34:13 (4th ed. 2018) ("The general rule is that for customs or usages to be recognized as binding by implication on parties to a contract, and as guides in the construction and interpretation of obligations and the performance of duties, they must be reasonable.").

351. *See* 21A AM. JUR. 2D *Customs and Usages* § 6, Westlaw (database updated Aug. 2018) ("[A] custom or usage must be general in its operation . . . .").

352. *See* Kenneth S. Abraham, *Custom, Noncustomary Practice, and Negligence*, 109 COLUM. L. REV. 1784, 1791–1804 (2009) (reviewing methodically these and other justifications for consulting custom when formulating tort duties of care).

353. Clarence Morris, *Custom and Negligence*, 42 COLUM. L. REV. 1147, 1148 (1942).

354. *See* Abraham, *supra* note 352, at 1798 ("[I]t is a common moral intuition that, other things being equal, it is unfair to punish someone for doing what everyone else does.").

355. *See* Gary Lawson, *The Rise and Rise of the Administrative State*, 107 HARV. L. REV. 1231 (1994).

the Mining Law of 1872,[356] rather than establishing a new federal standard for prospectors to stake a claim to a new mine, adopted "the local customs or rules of miners in the several mining districts" as their guide.[357] The basic structure of the law remains in force and is highly controversial.[358]

Regulators today also find it desirable to harmonize legal rules with existing industry custom. This is the philosophy behind ascendant "new governance" philosophies that strive to create regulatory partnerships between government and the private sector.[359] Government agencies using the well-known "responsive regulation" model prioritize engagement with industry to develop a shared understanding of appropriate behavior, turning to adversarial and punitive measures only when these efforts fail.[360] In the United States, privacy regulators such as the FTC consistently use the techniques of responsive regulation.[361] As we have seen, this includes extensive dialogue with industry and the incorporation of existing data security standards into their frameworks.[362]

The argument for absorption of industry practice into legal duties carries particular force where an expert profession has already developed a robust common understanding of that duty. Just as tort law uses the existing standards of medical practice to determine liability,[363] regulators also borrow from professional standards.

The strong influence of Generally Accepted Accounting Practices (GAAP) provides an excellent example. GAAP are the

356. Act of May 10, 1872, ch. 152, § 1, 17 Stat. 91 (codified as amended at 30 U.S.C. §§ 22–42 (2017)).

357. 30 U.S.C. § 22.

358. *See* CONG. RESEARCH SERV., RL33908, MINING ON FEDERAL LANDS: HARDROCK MINERALS (2009) (discussing arguments for changes in the Mining Law of 1872); Mark Squillace, *The Enduring Vitality of the General Mining Law of 1872*, 18 ENVTL. L. REP. 10261 (1988) (discussing congressional changes to the Mining Law of 1872).

359. *See generally* Orly Lobel, *The Renew Deal: The Fall of Regulation and the Rise of Governance in Contemporary Legal Thought*, 89 MINN. L. REV. 342 (2004) (discussing the strengths of regulatory partnerships between the government and private sector actors).

360. *See* IAN AYRES & JOHN BRAITHWAITE, RESPONSIVE REGULATION 35–48 (1992).

361. *See* McGeveran, *supra* note 8, at 997–1003 (discussing the FTC's application of the responsive regulation model).

362. *See supra* notes 70–75 and accompanying text.

363. *See* RESTATEMENT (SECOND) OF TORTS § 299A cmt. b (AM. LAW INST. 1965).

principles adopted by the Financial Accounting Standards Board (FASB), a nongovernmental professional organization, which the SEC considers authoritative.[364] Like the duty of data security, GAAP is explicitly principles-based rather than providing bright-line rules and is rooted in reasonableness.[365]

Basic institutional competence favors regulators' reliance on the industry-driven development of GAAP. Congress certainly lacks the expertise to develop such standards. Leading corporate law scholar John Coffee has put the point rather pungently, stating, "Congress has no more business legislating laws of accounting than it does legislating a law of gravity. But it can create a neutral and independent body to promulgate substantive accounting rules."[366] FASB establishes GAAP using formal procedural rules designed to solicit broad participation from a range of accounting experts and to uphold due process.[367] By empowering the profession to generate its own standards, government can achieve better compliance and ensure that the rules are not unduly onerous or unrealistic.

That said, GAAP does not control every legal dispute where financial records are at issue. It depends whether the policy rationale underlying the dispute is consistent with GAAP's policy rationale. The Supreme Court rejected the argument that tax adjudication must conform to GAAP, citing the different purposes of unambiguous revenue regulations and principles-based accounting standards.[368] The Medicare program's regulations require hospitals to use widely accepted industry accounting standards in keeping their books, but Medicare reimbursement decisions based on those records do not necessarily conform to

364. *See* Ganino v. Citizens Util. Co., 228 F.3d 154, 159 n.4 (2d Cir. 2000) (affirming the authoritative status of GAAP); Mary Michel, *Generally Accepted Accounting Principles (GAAP)*, *in* 1 ENCYCLOPEDIA OF AMERICAN BUSINESS HISTORY 181, 181–82 (Charles R. Geisst ed., 2006) (explaining the history and role of GAAP); *About the FASB*, FASB—FIN. ACCT. STANDARDS BOARD, http://www.fasb.org/jsp/FASB/Page/SectionPage&cid=1176154526495 (last visited Nov. 20, 2018) (stating the history and role of the FASB).

365. *See* Thor Power Tool Co. v. Comm'r, 439 U.S. 522, 544 (1979) ("[GAAP] tolerate[s] a range of 'reasonable' treatments, leaving the choice among alternatives to management.").

366. John C. Coffee, Jr., *Understanding Enron: "It's About the Gatekeepers, Stupid"*, 57 BUS. L. 1403, 1417 n.57 (2002).

367. *See* FIN. ACCOUNTING STANDARDS BD., RULES OF PROCEDURE 2 (2014).

368. *See Thor Power Tool Co.*, 439 U.S. at 542–43 ("Given this diversity, even contrariety, of objectives, any presumptive equivalency between tax and financial accounting would be unacceptable.").

GAAP.[369] And in securities fraud prosecutions, the degree of adherence to GAAP may serve as evidence concerning a defendant's good faith belief in the accuracy of financial statements, but it is not conclusive on the ultimate question of guilt.[370]

Like GAAP, many of the data security frameworks derived from private sources memorialize the wisdom of the profession about best practices. Financial control frameworks, such as the PCI DSS and the FINRA regulations, do so especially clearly because they are tied to a particular highly regulated industry.[371] Indeed, state lawmakers' deference to the PCI DSS resembles the SEC's authorization of GAAP.[372] The participatory stakeholder process leading to the development of the NIST Framework[373] also resembles the FASB's stakeholder consultations.

Thus, reliance on emerging industry best practices as the source for a duty of data security follows exactly the path the law has trod innumerable times before. This is an extensively tested method of creating legal duties. The reason it has been so common is that it has been found effective.

C. CALIBRATED TO RISK AND RESOURCES

The NIST Framework is very clear about the appropriate measure of cybersecurity investment and its relationship to other goals: "Prioritizing the mitigation of gaps is driven by the organization's business needs and risk management processes. This risk-based approach enables an organization to gauge the resources needed (e.g., staffing, funding) to achieve cybersecurity goals in a cost-effective, prioritized manner."[374]

The other frameworks discussed in Part I likewise embrace this emphasis on risk-informed cost-effectiveness. Even HIPAA, generally considered one of the more onerous of the traditional legal frameworks in Part I.A, predicates all the standards in the

369. *See* Shalala v. Guernsey Mem'l Hosp., 514 U.S. 87, 93–94 (1995).

370. *See* United States v. Rigas, 490 F.3d 208, 220 (2007) ("GAAP neither establishes nor shields guilt in a securities fraud case. . . . Instead, compliance with GAAP is relevant only as evidence of whether a defendant acted in good faith." (citing United States v. Simon, 425 F.2d 796, 805–06 (2d Cir. 1969))).

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

372. *See supra* notes 174–75 and accompanying text. Some states choose not to legislate in the area, a few simply absorb the PCI DSS into their statutes, but no state simply disregards the PCI DSS in favor of its own inconsistent framework.

373. *See supra* note 127 and accompanying text.

374. NIST Framework, *supra* note 126, at 11.

Security Rule on a principle of "flexibility of approach," under which regulated parties may "use any security measures that allow [them] to reasonably and appropriately implement the standards and implementation specifications . . . ."[375]

Like the features discussed in the previous two Sections, this is hardly new. Various forms of rough cost-benefit analysis have long been central to the development of liability rules and their associated duties.

Just about every first-year law student encounters the famous decision in *United States v. Carroll Towing Co.*[376] during the standard tort law course.[377] The case involved an accidental sinking of a barge in New York Harbor.[378] A key issue in the case was whether the owner of the barge was negligent for failing to have an attendant on duty at the time of the accident.[379] Judge Learned Hand, probably the most influential American judge outside the U.S. Supreme Court in the middle of the twentieth century, used the case to articulate a formula for determining legal responsibility in situations where a risk was foreseeable:

> Since there are occasions when every vessel will break from her moorings, and since, if she does, she becomes a menace to those about her; the owner's duty, as in other similar situations, to provide against resulting injuries is a function of three variables: (1) The probability that she will break away; (2) the gravity of the resulting injury, if she does; (3) the burden of adequate precautions. Possibly it serves to bring this notion into relief to state it in algebraic terms: if the probability be called P; the injury, L; and the burden, B; liability depends upon whether B is less than L multiplied by P: i.e., whether $B < PL$.[380]

Judge Hand's resort to algebra in *Carroll Towing* is a bit ridiculous, of course. Judge Richard Posner—probably Judge Hand's successor later in the twentieth century as the most influential judge not on the Supreme Court—has wryly noted, "the Hand formula does not yield mathematically precise results in practice."[381]

375. 45 C.F.R. § 164.306(b)(1) (2017).

376. 159 F.2d 169 (2d Cir. 1947).

377. *See* Patrick J. Kelley, *The* Carroll Towing Company *Case and the Teaching of Tort Law*, 45 ST. LOUIS U. L.J. 731, 732 (2001) (surveying coverage of torts casebooks and concluding that "each casebook gives the *Carroll Towing Co.* formula a prominent place in its treatment of the standard of conduct in negligence cases").

378. *Carroll Towing*, 159 F.2d at 170–71.

379. *Id.*

380. *Id.* at 173.

381. U.S. Fid. & Guar. Co. v. Jadranska Slobodna Plovidba, 683 F.2d 1022, 1026 (7th Cir. 1982).

Nonetheless, this simple equation has been known as the "Hand Formula" or "Hand Test" ever since, and it has been characterized by some as the germinal seed of cost-benefit analysis in modern law.[382] *Carroll Towing* may not be as influential in workaday tort law as its prominence in law school casebooks would suggest.[383] But even though juries seldom use the Hand Test when actually deciding individual cases, judges frequently cite it in their discussion of the broader theory of negligence.[384]

The Hand Test has proven a useful simple heuristic for constructing the boundaries of liability in cases of "foreseeable unreasonable risk."[385] Security breaches in large networked databases, like drifting barges in busy wartime harbors, are predictable and serious hazards. The crucial question is determining when to impose a duty to prevent that harm. If money were no object, the answer would be "always." Because resources are limited, however, we need a way to ascertain what degree of safeguards should be required by law. Hindsight bias can present a serious problem when judging the reasonableness of precautions ex post, after a breach has occurred.[386] But Judge Hand's instruction to balance the burden of precautions (B) against the probability of a mishap (P) and the severity of the resulting harm (L) ameliorates this tendency by ensuring proper attention to resources. This leads to the sorts of risk assessment that have become common in data security law.

Consider once again the "flexibility of approach" at the center of the HIPAA Security Rule, and see how it maps on to the Hand Test. Items (i)-(iii) on this list capture B from the Hand Test, and item (iv) counterbalances them with combined consideration of PL:

> In deciding which security measures to use, a covered entity or business associate must take into account the following factors:
>
> (i) The size, complexity, and capabilities of the covered entity or business associate.

382. *See infra* note 383 (discussing the relevance of *Carroll Towing* within the negligence jurisprudence).

383. *See* Kelley, *supra* note 377, at 757.

384. *See* Stephen G. Gilles, *The Invisible Hand Formula*, 80 VA. L. REV. 1016, 1018 (1994) (discussing the rare use of the Hand test in jury instructions).

385. *See id.* at 1019.

386. *See generally* Kim A. Kamin & Jeffrey J. Rachlinski, *Ex Post ≠ Ex Ante: Determining Liability in Hindsight*, 19 LAW & HUM. BEHAV. 89 (1995) (describing an experiment in which decisions about risk and precaution were judged much more harshly ex post than ex ante).

> (ii) The covered entity's or the business associate's technical infrastructure, hardware, and software security capabilities.
>
> (iii) The costs of security measures.
>
> (iv) The probability and criticality of potential risks to electronic protected health information.[387]

The three-part test for the FTC to proceed against unfairness under Section 5 also incorporates Judge Hand's variables; for an act to be unfair, the statute requires that it is "likely [P] to cause substantial injury to consumers which is not reasonably avoidable by consumers themselves [L] and not out-weighed by countervailing benefits to consumers or to competition [B]."[388]

Security professionals emulate the Hand Formula just as much as lawmakers do. For example, the CISSP guide explains the "Probability x Damage Potential" ranking, which assigns ratings between one and ten for those two variables, as one potential risk assessment methodology.[389] Data custodians are told they should prioritize threats with higher scores under this close cousin of *Carroll Towing*—and furthermore, "[t]echnologies and processes to remediate threats should be considered and weighed according to their cost and effectiveness."[390]

In the *Wyndham* case, the Third Circuit viewed the FTC's power as an expression of a cost-benefit analysis — a descendent of the Hand Formula.[391] The court concluded that the FTC's authorizing statute, "informs parties that the relevant inquiry here is a cost-benefit analysis that considers a number of relevant factors, including the probability and expected size of reasonably unavoidable harms to consumers given a certain level of cybersecurity and the costs to consumers that would arise from investment in stronger cybersecurity."[392] This conclusion adheres to Judge Hand's simple formula, balancing the likelihood and severity of harm against the burden of precautions.[393] Wide recognition that the harm is both serious and likely means robust protective measures are in order. In other words, failure to adopt such precautions in these cases would be unreasonable, and that is a violation of the duty of data security.

387. 45 C.F.R. § 164.306(b)(2) (2017).
388. 15 U.S.C. § 45(n) (2017).
389. *See* STEWART, *supra* note 193, at 34–35.
390. *Id.* at 35.
391. FTC v. Wyndham Worldwide Corp., 799 F.3d 236, 255 (3d Cir. 2015).
392. *Id.* (citations omitted).
393. *See* United States v. Carroll Towing Co., 159 F.2d 169, 173 (2d. Cir. 1947) (explaining the Hand formula).

CONCLUSION

The fourteen frameworks reviewed in this Article have converged around a developing consensus concerning the duty of data security. The different sources of law sound in harmony, not cacophony. Claims that law provides no guidance to data custodians are balderdash.

The duty of data security requires that data custodians assess their security risks and implement a policy that responds to that risk. The resulting compliance program must incorporate sensible architectural controls on access and avoid certain specified worst practices. The duty of data security is expressed in standards rather than rules, is rooted in professional best practices, and is consistent with a risk-benefit analysis. As always in the law—whether in torts, consumer protection law, or responsive regulation—the expectation is reasonableness, not perfection.

Does all this tell a company's CISO exactly what to do, like a cookbook recipe? No, it does not. And that is as it should be. Like industrial safety, medical care, or accounting procedures, data security is complex, contextual, and increasingly professionalized. The duty of data security provides the type of flexible guidance that allows data custodians to use sound judgment and reduce (but not eliminate) the risk of breach. This is how the law has worked for centuries. It got us this far, and it will serve us well in confronting the challenges of data security in a digital age.