# HACKING CYBERSECURITY LAW

*Jeff Kosseff*[*]

*Unlike discrete legal fields such as patent and copyright law, cybersecurity law spans a number of sections of the U.S. Code, as well as state and international laws. Because the contours of cybersecurity law are blurry, U.S. policymakers have not sufficiently determined how to most effectively align statutes and regulations with current cybersecurity threats. This Article builds on the author's previous work to define the scope of cybersecurity law and suggests seven guiding principles to radically reshape—or "hack"—the legal system to better address current and future cybersecurity threats. This Article draws on legal scholarship and other fields of law to derive high-level goals for policymakers as they seek to make cybersecurity law more effective, cohesive, and agile.*

TABLE OF CONTENTS



[*] Assistant Professor, Cyber Science Department, United States Naval Academy, Annapolis, MD. J.D., Georgetown University Law Center. M.P.P., B.A., University of Michigan. The views expressed in this Article are only the author's and do not reflect the views of the Naval Academy, Department of Navy, or Department of Defense. Thanks to Ido Kilovaty and Scott Shackelford for very helpful comments on an earlier draft.

## I. INTRODUCTION

Cybersecurity is one of the most vexing challenges for U.S. policymakers. Inadequate security of computers, networks, systems, and data can devastate the economy,[1] upend the lives of individuals,[2] weaken national security,[3] and even undercut the foundations of our democratic system.[4] Individuals, businesses, and governments of all levels share a common interest in bolstering collective cybersecurity. The United States continues to face persistent threats to public and private infrastructure from increasingly sophisticated and determined adversaries, making it more urgent than ever for the nation to develop a whole-of-nation response.

The United States has made great strides on some aspects of its cyber strategy to better address these threats. For instance, the Defense Department in 2018 announced a "persistent engagement" strategy, which recognizes that cyber threats are continuous, and not episodic events.[5] The military strategy includes an operational concept known as "defend forward," in which the United States will conduct operations outside of military operations with the goal of positioning to degrade cyber operations, gather information about threats, and influence adversaries to cease their activities directed toward the United States.[6]

While the United States has progressed on its military strategy by becoming more aggressive in cyberspace, that is only part of the equation. Equally important to combatting the persistent threats is improving domestic cybersecurity.

1. *See* Herb Weisbaum, *The Total Cost of a Data Breach–Including Lost Business–Keeps Growing*, NBC NEWS (July 30, 2018, 2:15 PM), https://www.nbcnews.com/business/consumer/total-cost-data-breach-including-lost-business-keeps-growing-n895826 ("The financial damage caused by a data breach has spiked by more than 6 percent since last year and now costs companies an average of $3.86 million each, according to a new study. Aside from expensive technical investigations and regulatory filings, a breach also includes hidden costs such as lost business, negative impact on reputation, and employee time spent on recovery, according to a new report by the Ponemon Institute.").

2. *See* Ryan Calo, *A Long-Standing Debate: Reflections on Risk and Anxiety: A Theory of Data Breach Harms by Daniel Solove and Danielle Keats Citron*, 96 TEX. L. REV. ONLINE 59, 60 (2018); *see also* Daniel J. Solove & Danielle Keats Citron, *Risk & Anxiety: A Theory of Data Breach Harms*, 96 TEX. L. REV. 737, 745 (2018).

3. *See* DANIEL R. COATS, SENATE SELECT COMMITTEE ON INTELLIGENCE, WORLDWIDE THREAT ASSESSMENT OF THE U.S. INTELLIGENCE COMMUNITY (2019) ("Our adversaries and strategic competitors will increasingly use cyber capabilities—including cyber espionage, attack, and influence—to seek political, economic, and military advantage over the United States and its allies and partners. China, Russia, Iran, and North Korea increasingly use cyber operations to threaten both minds and machines in an expanding number of ways—to steal information, to influence our citizens, or to disrupt critical infrastructure.").

4. *See* Eric Lipton et al., *The Perfect Weapon: How Russian Cyberpower Invaded the U.S.*, N.Y. TIMES (Dec. 13, 2016), https://www.nytimes.com/2016/12/13/us/politics/russia-hack-election-dnc.html ("While there's no way to be certain of the ultimate impact of the hack, this much is clear: A low-cost, high-impact weapon that Russia had test-fired in elections from Ukraine to Europe was trained on the United States, with devastating effectiveness. For Russia, with an enfeebled economy and a nuclear arsenal it cannot use short of all-out war, cyberpower proved the perfect weapon: cheap, hard to see coming, hard to trace.").

5. *See* Michael P. Fischerkeller & Richard J. Harknett, *Persistent Engagement and Tacit Bargaining: A Path Toward Constructing Norms in Cyberspace*, LAWFARE (Nov. 9, 2018, 7:00 AM), https://www.lawfareblog.com/persistent-engagement-and-tacit-bargaining-path-toward-constructing-norms-cyberspace ("Persistent engagement recognizes that cyberspace's structural feature of interconnectedness and its core condition of constant contact creates a strategic necessity to operate continuously in cyberspace.").

6. *See id.*

This task is particularly challenging, as much of the infrastructure and data that adversaries target is controlled by the private sector.[7] Breaches that targeted Sony, Yahoo, the Democratic National Committee, and so many other nongovernment organizations have severe consequences for the economy and national security. Accordingly, any national cybersecurity strategy must account for—and, ideally, influence—the cybersecurity of the private sector.

The government's most powerful lever for influencing the private sector is its lawmaking. Whether through carrots—such as technological assistance, education, tax credits, or sticks—such as regulations and private causes of action, U.S. laws can help to shape that behavior.

Unfortunately, the cluster of state and federal laws that could be broadly considered to be U.S. "cybersecurity law" are outdated—often decades old—and in many cases lack a common purpose to address the current cybersecurity threats. I have broadly described these laws in a 2018 article, *Defining Cybersecurity Law*.[8] In that article, I explain how laws related to data security, computer hacking, consumer protection, and privacy can broadly be considered part of "cybersecurity law," and I highlight areas where they are lacking.[9]

This Article builds on that research and sets forth guiding principles for policymakers to hack cybersecurity law. By "hacking," I do not mean the type of unauthorized access to computers that is covered under the Computer Fraud and Abuse Act (which is one of the many statutes that I include in my definition of cybersecurity law). Instead, I refer to another definition of hacking: taking a bold move that is intended to improve something; as Merriam-Webster defines the term: "to cut or shape by or as if by crude or ruthless strokes."[10] Cybersecurity laws are so misaligned with current threats and challenges that policymakers cannot fix them through modest refinements or amendments.

A radical rethinking and overhaul is necessary. Crude strokes. Ruthless strokes.

A hacking.

This hacking can include new statutes, new regulations, new guidance, and even new exercise of authorities under existing statutes and regulations. The ultimate goal is to better align the legal rules—particularly those that govern private sector cybersecurity—with methods that effectively combat existing and future cybersecurity challenges.

Part II of this Article provides a brief overview of the various types of laws that broadly encompass "cybersecurity law" under my definition of the field. Part

7. *See* Chuck Brooks, *Public Private Partnerships and the Cybersecurity Challenge of Protecting Critical Infrastructure*, FORBES (May 6, 2019, 1:24 AM), https://www.forbes.com/sites/cognitiveworld/2019/05/06/public-private-partnerships-and-the-cybersecurity-challenge-of-protecting-critical-infrastructure/#cd555b25a577 ("In the U.S., most of the critical infrastructure, including defense, oil and gas, electric power grids, health care, utilities, communications, transportation, education, banking and finance, is owned by the private sector (about 85 percent according to DHS) and regulated by the public sector.").

8. Jeff Kosseff, *Defining Cybersecurity Law*, 103 IOWA L. REV. 985 (2018) [hereinafter *Defining Cybersecurity Law*].

9. *Id.*

10. *Hack*, MERRIAM-WEBSTER'S COLLEGIATE DICTIONARY (11th ed. 2004).

III suggests seven principles to guide U.S. policymakers as they work to hack cybersecurity laws. I developed these principles by drawing on literature that documents areas of success in cybersecurity law and other areas of the law in which the government has attempted to influence private sector behavior. I also account for the unique nature of cybersecurity threats, including the alignments of incentives within the private sector. Those principles are:

> **1. Informed:** Congress, regulatory agencies, executive branch officials, and courts must have a clear and current understanding of the technology and cybersecurity threats and potential solutions *before* they develop or modify legal rules.
>
> **2. Clear:** To the greatest extent possible, the private sector must have a clear understanding of their requirements under cybersecurity law.
>
> **3. Adaptive:** While some cybersecurity laws can include generalizable standards that are easily adaptable to new challenges, others simply fail to anticipate future technology and its cybersecurity impacts. In such cases, Congress should empower a regulatory agency to promulgate regulations that adapt to the new technological reality.
>
> **4. Comprehensive:** Cybersecurity laws often are conflated with privacy laws, as there is significant overlap. Cybersecurity laws, however, must address more than just the confidentiality of personal information, and also seek to protect from unauthorized alteration of data and attacks such as ransomware that cause data or systems to become unavailable. Cybersecurity laws also must focus not just on financial harms, but any threats to national security or individual privacy or safety.
>
> **5. Cohesive:** Companies currently face a web of requirements at the state levels, and many of these requirements conflict. Governments should attempt, to the greatest extent possible, to align the requirements nationally, in an effort to provide a clear regulatory framework.
>
> **6. Global:** Just as it is necessary for a unified national policy, global coordination of cybersecurity regulations and incentives will help to improve the overall efficacy of fighting threats that do not adhere to traditional geographic borders.
>
> **7. Collaborative:** A number of federal agencies specialize in cybersecurity. The experts in these agencies should work together, rather than in separate silos. These collaborative efforts should stress not only punitive measures, such as criminal enforcement and regulation, but also partnerships such as threat information sharing.

These aspirational principles are drawn from nearly a decade of practicing cybersecurity law, teaching the subject, and writing articles and a textbook on the topic. What has become clear in my experience so far is that there is not a unified set of principles from which lawmakers and public officials may draw as they develop cybersecurity law and policy. This Article is my attempt to suggest these guiding, high-level principles.

## II. THE BROAD SCOPE OF CYBERSECURITY LAW

In *Defining Cybersecurity Law*, I reviewed caselaw, statutes, and technical literature to arrive at a broad definition of cybersecurity law:

"Cybersecurity law promotes the confidentiality, integrity, and availability of public and private information, systems, and networks, through the use of forward-looking regulations and incentives, with the goal of protecting individual rights and privacy, economic interests, and national security."[11]

This field is not easily definable, as it includes not only data security laws, but other criminal and civil statutes that shape cybersecurity, as well as common law claims that arise in litigation after data breaches. Among the categories of regulations, statutes, and common-law rules that fall under this definition, as outlined more fully in *Defining Cybersecurity Law*:

**State Data Security and Cybersecurity Statutes:** More than twenty states have enacted data security statutes.[12] Of those state laws, thirteen merely require "reasonable" protection or policies for the personal information of those states' residents. The data security laws in Alabama,[13] Oregon,[14] Rhode Island,[15] Nevada,[16] and Massachusetts[17] require or suggest specific safeguards, such as encryption. Ohio's data security law provides companies with an affirmative defense to data breach tort claims, provided that they have complied with a specified cybersecurity standard.[18] The New York Department of Financial Services in 2017 finalized comprehensive cybersecurity regulations for its regulated companies,[19] and the rules have been hailed for their rigor and comprehensive scope.[20]

**Federal Data Security Laws:** Unlike these state governments, the federal government does not have a general statute that explicitly requires security of personal information across all industries and sectors. Nonetheless, the Federal Trade Commission (the "FTC" or the "Commission") provides some data security and privacy regulation under Section 5 of the Federal Trade Commission Act,

11. *Defining Cybersecurity Law*, *supra* note 8, at 1010.

12. For a full list, see *Data Security Laws | Private Sector*, NAT'L CONFERENCE OF STATE LEGISLATURES (May 29, 2019), www.ncsl.org/research/telecommunications-and-information-technology/data-security-laws.aspx.

13. S. 318, 2018 (Ala. 2018) (to be codified).

14. OR. REV. STAT. ANN. § 646A.622(1) (West 2018) ("A person that owns, maintains or otherwise possesses, or has control over or access to, data that includes personal information that the person uses in the course of the person's business, vocation, occupation or volunteer activities shall develop, implement and maintain reasonable safeguards to protect the security, confidentiality and integrity of the personal information, including safeguards that protect the personal information when the person disposes of the personal information.").

15. 11 R.I. GEN. LAWS ANN. § 49.3-2(a) (West 2019).

16. NEV. REV. STAT. ANN. § 603A.210 (LexisNexis 2019).

17. MASS. ANN. LAWS ch. 93H, § 2(a) (LexisNexis 2019).

18. OHIO REV. CODE ANN. §§ 1354.01–.05 (LexisNexis 2019).

19. N.Y. COMP. CODES R. & REGS. tit. 23, §§ 500.00–.23 (2019).

20. *New York Cyber Regulations to Impose New and Significant Burdens on the Financial Services Industry*, PRIVACY IN FOCUS (Wiley Rein LLP), Jan. 2017 ("While the final version may still change modestly, this proposal will impose significant new compliance obligations on the financial services industry, with a relatively short compliance timetable.").

which prohibits "unfair or deceptive acts or practices in or affecting commerce."[21] The FTC has brought dozens of enforcement actions against companies that allegedly lied about their data security practices or failed to reasonably safeguard personal information.[22] In 2015, the U.S. Court of Appeals for the Third Circuit affirmed the FTC's authority to bring such claims under Section 5's "unfairness" prong,"[23] but in 2018 the U.S. Court of Appeals for the Eleventh Circuit vacated an FTC cease-and-desist order issued under the statute, concluding that it failed to adequately articulate data security standards.[24] Congress has passed more specific data security standards for particular sectors, such as the Gramm-Leach-Bliley Act for financial institutions[25] and the Health Insurance Portability and Accountability Act for health plans, healthcare clearinghouses, healthcare providers, and their business associates.[26]

**Data Breach Notification Laws:** Every state and the District of Columbia have passed statutes that require companies to notify their residents if certain forms of personal information have been accessed or acquired by unauthorized parties.[27] The requirements vary, with states defining "personal information" differently, and mandating particular forms and type of notice. Some laws require notice to regulators, law enforcement, or credit bureaus. The requirements also may conflict. Massachusetts, for instance, prohibits companies from describing how a data breach occurred,[28] while other states require a brief description of the incident.[29] Some states only require notice if the business determines that there is a reasonable likelihood of harm,[30] while others require notification regardless of the determination of likelihood of harm.[31] Some states require companies to notify state regulators of data breaches,[32] while others do not.[33] Breach notice laws apply to companies regardless of whether they are physically located in the

21. 15 U.S.C. § 45(a)(1) (2018).

22. *See Cases Tagged with Data Security*, FED. TRADE COMM'N, https://www.ftc.gov/enforcement/cases-proceedings/terms/249 (last visited Mar. 23, 2020).

23. FTC v. Wyndham Worldwide Corp., 799 F.3d 236, 247 (3d Cir. 2015) ("We are therefore not persuaded by Wyndham's arguments that the alleged conduct falls outside the plain meaning of 'unfair.'").

24. LabMD, Inc. v. Fed. Trade Comm'n, 894 F.3d 1221, 1237 (11th Cir. 2018) ("[The cease and desist order] does not enjoin a specific act or practice. Instead, it mandates a complete overhaul of LabMD's data-security program and says precious little about how this is to be accomplished. Moreover, it effectually charges the district court with managing the overhaul. This is a scheme Congress could not have envisioned.").

25. 15 U.S.C. § 6801 (2018).

26. 44 U.S.C. §§ 3541–3549 (2018).

27. *See Security Breach Notification Laws*, NAT'L CONFERENCE OF STATE LEGISLATURES (Mar. 8, 2020), http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx.

28. MASS. ANN. LAWS ch. 93H (LexisNexis 2019).

29. *See, e.g.*, IOWA CODE § 715C.2 (2019) (requiring data breach notices to include a "description of the breach of security.").

30. *See, e.g.*, MICH. COMP. LAWS ANN. § 445.72 (West 2019) (requiring notice unless the organization determines that "the security breach has not or is not likely to cause substantial loss or injury to, or result in identity theft with respect to, 1 or more residents of this state[.]").

31. *See, e.g.*, CAL. CIV. CODE § 1798.82 (West 2019).

32. *See, e.g.*, ALASKA STAT. ANN. §§ 45.48.010 (West 2019).

33. *See, e.g.*, 815 III. COMP. STAT. ANN. 530/1 (West 2019).

state,[34] though some apply only to companies that "conduct business" in that state.[35] But even the latter category of breach notice law can apply to a wide range of companies that are not headquartered or physically present in the state, as "doing business" or "conducting business" is a broad term that can be triggered even by remote transactions.[36] Effectively, that means that even mid-sized companies may be subject to all fifty-one state breach notice laws, as the main determinant of a law's applicability is the location of the individual whose data was breached.[37]

**Data Breach Litigation:** Increasingly, companies have faced class action lawsuits from private parties arising from data breaches.[38] Companies have faced claims under state common-law theories such as negligence.[39] Plaintiffs also sue under state consumer protection statutes,[40] many of which allow private plaintiffs to bring suits for unfair or deceptive trade practices (the FTC Act, in contrast, does not provide for private litigation). Plaintiffs also may sue for breach of contract.[41]

**Computer Hacking Laws:** In addition to regulating the security practices of companies, a number of federal and state laws impose criminal and civil liability on individuals who cause damage to computers, obtain information without authorization, or otherwise engage in what can broadly be described as unauthorized "hacking."[42] These include the Computer Fraud and Abuse Act,[43] state

34. *See, e.g.*, IOWA CODE § 715C.2 (2019) ("Any person who owns or licenses computerized data that includes a consumer's personal information that is used in the course of the person's business, vocation, occupation, or volunteer activities and that was subject to a breach of security shall give notice of the breach of security . . . .").

35. *See, e.g.*, CAL. CIV. CODE § 1798.82 (West 2019) ("A person or business that conducts business in California, and that owns or licenses computerized data that includes personal information, shall disclose a breach of the security of the system following discovery or notification of the breach in the security of the data to a resident of California . . . .").

36. *See* Lothar Determann, *Analysis: The California Consumer Privacy Act of 2018*, INT'L ASS'N OF PRIVACY PROFS., https://iapp.org/news/a/analysis-the-california-consumer-privacy-act-of-2018/ (last visited Mar. 23, 2020) ("Most U.S. companies will find it difficult to determine that they are not doing business in the state of California, because the term 'doing business' is understood very broadly.").

37. *See* MARK L. KROTOSKI, LUCY WANG & JENNIFER S. ROSEN, BLOOMBERG BNA, THE NEED TO REPAIR THE COMPLEX, CUMBERSOME, COSTLY DATA BREACH NOTIFICATION MAZE 2 (2016) ("[E]ven though the company operates nationally and its security systems are managed centrally, the company must tailor each notification to fit the specific requirements of the state in which each customer resides."); Jennifer Martin & Chimene I. Keitner, *Regulating Data Privacy in an Interconnected World—How Far Does California's New Law Reach?*, BLOOMBERG L. NEWS (July 18, 2019, 1:46 PM), https://news.bloomberglaw.com/white-collar-and-criminal-law/insight-regulating-data-privacy-in-an-interconnected-worldhow-far-does-californias-new-law-reach ("Most state law privacy initiatives define their coverage based at least in part on the identity of the user (or 'data subject') rather than the physical location of the company.").

38. *See* Fernando M. Pinguelo, Angelo A. Stio III & Hasan Ibrahim, *Even as Data Breaches Continue to Increase, Obstacles Remain for Litigants Seeking to Pursue Securities Fraud and Derivative Suits*, N.J. LAW., Apr. 2018, at 40.

39. *See, e.g.*, Hutton v. Nat'l Bd. Of Examiners in Optometry, Inc., 892 F.3d 612, 616 (4th Cir. 2018).

40. *In re* Yahoo! Customer Data Security Breach Litigation, 313 F. Supp. 3d 1113, 1128 (N.D. Cal. 2018).

41. *Id.* at 1136.

42. *See Computer Crime Statutes*, NAT'L CONFERENCE OF STATE LEGISLATURES (Feb. 24, 2020), https://www.ncsl.org/research/telecommunications-and-information-technology/computer-hacking-and-unauthorized-access-laws.aspx.

43. 18 U.S.C. § 1030 (2018).

hacking laws, the Economic Espionage Act,[44] and Section 1201 of the Digital Millennium Copyright Act.[45]

**Public-Private Partnerships:** Although much of the focus of cybersecurity law involves the regulation of private behavior, the U.S. government has made some attempts to partner with the private sector to achieve a shared goal of cybersecurity.[46] Most notably, the Cybersecurity Act of 2015 provides limited immunity for companies to share cybersecurity threat indicators and defensive measures with the federal government and other entities.[47] The Department of Homeland Security coordinates threat-sharing with the private sector,[48] and the National Institute of Standards and Technology has developed a cybersecurity framework and a number of cybersecurity standards that are widely used throughout the public and private sectors.[49]

Many of these laws have been on the books for many decades, and have not been substantially updated to account for the many technological changes of the modern Internet era.[50] *Defining Cybersecurity Law* sought to define the full range of laws that can be considered under the umbrella of cybersecurity, and to identify the goals of cybersecurity law.[51] This Article is a logical next step of that work, identifying principles that should guide policymakers as they attempt to modernize those laws and align them with the current and future cybersecurity landscape.

Standing alone, many of these laws serve important functions. For instance, the Computer Fraud and Abuse Act, though rightly criticized for its ambiguity,[52] continues to play a vital role both in prosecuting computer criminals and allowing hacking victims to bring civil lawsuits against perpetrators.[53] Likewise, the Department of Homeland Security continues to work to implement the Cybersecurity Act of 2015 and better share cyber-threat information.[54] And the FTC has brought dozens of data security enforcement actions against companies despite its relatively limited statutory authority.[55] The primary systemic problem in the

44. 18 U.S.C. §§ 1831–1839 (2018).

45. 17 U.S.C. § 1201 (2018).

46. *See, e.g.*, *About Us: CISA*, U.S. DEP'T OF HOMELAND SEC., https://www.us-cert.gov/about-us (last visited Mar. 23, 2020).

47. 6 U.S.C. § 1505(b) (2018).

48. *See About Us: CISA*, *supra* note 46.

49. *See* NAT'L INST. OF STANDARDS AND TECH., FRAMEWORK FOR IMPROVING CRITICAL INFRASTRUCTURE CYBERSECURITY (2018), https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf.

50. *Defining Cybersecurity Law*, *supra* note 8, at 988.

51. *Id.*

52. *See* Andrea Matwyshyn, *The Law of the Zebra*, 28 BERKELEY TECH. L.J. 155, 173 (2013).

53. *See, e.g.*, Criminal Charges Filed in Los Angeles and Alaska in Conjunction with Seizures of 15 Websites Offering DDoS-For-Hire Services, U.S. DEP'T OF JUSTICE (Dec. 20, 2018), https://www.justice.gov/opa/pr/criminal-charges-filed-los-angeles-and-alaska-conjunction-seizures-15-websites-offering-ddos.

54. *See* Jory Heckman, *DHS Launches One-Stop Shop for Cyber Threat Sharing with Private Sector*, FED. NEWS NETWORK (July 31, 2018, 3:47 PM), https://federalnewsnetwork.com/cybersecurity/2018/07/dhs-launches-one-stop-shop-for-cyber-threat-sharing-with-private-sector/.

55. *See* FED. TRADE COMM'N, FEDERAL TRADE COMMISSION, PRIVACY & DATA SECURITY UPDATE: 2018 3 (2019), https://www.ftc.gov/system/files/documents/reports/privacy-data-security-update-2018/2018-privacy-data-security-report-508.pdf ("The Commission has brought hundreds of enforcement actions protecting the privacy of consumer information. Its enforcement actions have addressed practices offline, online, and in the mobile

United States, however, is that few policymakers have stepped back to consider how all of these components function as a whole, and how to improve the entire system to better meet the nation's cybersecurity challenges. This Article sets forth guiding principles to serve as a starting point for this vital discussion.

At the outset, it is important to note that this Article does *not* suggest that the United States should tear down its cybersecurity legal system and start over. This would be unwise for a few reasons. First, in the age of political gridlock, a massive overhaul of every cybersecurity law seems highly unlikely. Second, many corporate cybersecurity practices are built on expectations from the existing system. And third, while many cybersecurity laws are flawed (and some deeply so), they often effectively address some discrete parts of our cybersecurity problems. Rather than a total overhaul, this Article suggests a tailored hacking that sharpens the current laws and supplements the major gaps and blind spots to more effectively address current and future threats.

## III. GUIDING PRINCIPLES FOR HACKING CYBERSECURITY LAW

In *Defining Cybersecurity Law*, I observed that "the patchwork of U.S. statutes and regulations that constitute cybersecurity is an uncoordinated mishmash of requirements that mostly were conceived long before modern cyberthreats."[56] The goal of the article was to provide a taxonomy for what we mean when we say "cybersecurity law," allowing for "coherence and a broad framework as scholars, policymakers, and legislatures evaluate our existing laws and consider new policies."[57] In short, the article argued there is an urgent need for a modernization of U.S. cybersecurity law.

This Article presents the next step to guide policymakers in meeting that goal. Rather than proposing a specific set of prescriptive policies, I instead articulate seven principles that should guide lawmakers and regulators as they determine how to align cybersecurity laws with the current threats.

### *A. Informed*

It should go without saying that lawmakers should debate and enact cybersecurity laws that are supported by science and are drafted by people who understand the underlying policy *and* technological issues. As Mark Fenwick, Wulf Kaal, and Erik Vermeulen recently wrote in an article about modern regulation, "In a data-based regulatory environment there is a clear need for measures that are built on flexible and inclusive processes that involve startups and established companies, regulators, experts and the public."[58]

environment. It has brought enforcement actions against well-known companies, such as Google, Facebook, Twitter, and Microsoft, as well as lesser-known companies.").

56. *Defining Cybersecurity Law*, *supra* note 8, at 988.

57. *Id.* at 1031.

58. Mark D. Fenwick et al., *Regulation Tomorrow: What Happens When Technology is Faster than the Law?*, 6 AM. U. BUS. L. REV. 561, 593 (2017) ("In an age of constant, complex and disruptive technological

Unfortunately, recent events call into question whether lawmakers and their staffers have an adequate grasp of the challenges and potential solutions.

Perhaps at no time was this clearer than April 2018, when the Senate Judiciary and Commerce Committees held a joint hearing on Facebook's privacy practices. For instance, Sen. Orrin Hatch asked Facebook CEO Mark Zuckerberg, "How do you sustain a business model in which users don't pay for your service?"[59]

"Senator, we run ads," Zuckerberg responded.[60]

The exchange became fodder for jokes, but it demonstrated a far deeper problem with the ability of Washington to develop effective rules for technology companies. Writing about the hearing for Vox, Emily Stewart observed that "[s]ome of the lines of questioning senators from both parties pursued demonstrated they aren't exactly the most tech-savvy bunch, aren't entirely clear on how Facebook works, or maybe have just never used the platform."[61] Sean Burch, writing in The Wrap, posited that "Orrin Hatch might not have the best understanding of Facebook."[62] Jessica Rosenworcel, a commissioner on the Federal Communications Commission, wrote that the hearings "made clear both how powerful new technologies are, and how important it is to have a common understanding of their basic mechanics."[63]

Of course, Congress has long faced criticism for being out of touch with technology. Perhaps most notoriously, at a 2006 Senate committee hearing, the late Sen. Ted Stevens offered this description of the Internet in a discussion about net neutrality: "The internet is not something that you just dump something on, it's not a big truck, it's, it's a series of tubes."[64]

If members of Congress are unable to understand the basic business model and data flow for a two billion-member social media site, how are they expected to develop effective and enduring laws that will improve the cybersecurity of social media and other technology? In June 2018, a group of academics (including this author), policymakers, and industry experts met at Georgetown Univer-

innovation, knowing what, when, and how to structure regulatory interventions has become more difficult. Regulators find themselves in a situation where they believe they must opt for either reckless action (regulation without sufficient facts) or paralysis (doing nothing).").

59. Emily Stewart, *Lawmakers Seem Confused About What Facebook Does—and How to Fix It*, VOX (Apr. 10, 2018, 7:50 PM), https://www.vox.com/policy-and-politics/2018/4/10/17222062/mark-zuckerberg-testimony-graham-facebook-regulations.

60. *Id.*

61. *Id.*

62. Sean Burch, *'Senator, We Run Ads': Hatch Mocked for Basic Facebook Question to Zuckerberg*, WRAP (Apr. 10, 2018, 1:24 PM), https://www.thewrap.com/senator-orrin-hatch-facebook-biz-model-zuckerberg/.

63. Jessica Rosenworcel, *The Facebook Hearings Demonstrate the Need for Technology Policy Experts in Congress*, NBC NEWS (Apr. 13, 2018, 3:44 AM), https://www.nbcnews.com/think/opinion/facebook-hearings-demonstrate-need-technology-policy-experts-congress-ncna865611.

64. Alex Gangitano, *Flashback Friday: 'A Series of Tubes'*, ROLL CALL (Feb. 16, 2018, 5:00 AM), https://www.rollcall.com/news/hoh/congressional-throwback.

sity Law Center to answer just this question. In a twenty-page report summarizing the discussion, the organizers noted the "broad recognition that Congress should be better equipped to understand technology."[65]

The Georgetown workshop focused on the need to revive the Office of Technology Assessment ("OTA"), which from 1972 until its defunding in 1995 was a small office within the legislative branch that employed scientists with the mission to equip Congress "with new and effective means for securing competent, unbiased information concerning the physical, biological, economic, social, and political effects of [technology] applications."[66]

The general sentiment of the group was that there is a need to bring back a nonpartisan office—whether OTA or another name—to provide informed technological advice to Congress. Peter Blair, a former OTA division head, outlined six evaluation criteria for such an entity:

**Authoritative:** "there must be direct and substantial involvement of the most knowledgeable and trusted experts."[67]

**Objectively informed:** "all important perspectives must be utilized and represented in a balanced way, and the advice should inform the debate rather than support one position or another."[68]

**Independent:** "free from vested interests, but aware and transparently informed by all of them."[69]

**Relevant:** "requests for advice, and the scope and scale of the issues to be resolved, ought to come from Congress, or at least involve some congressional governance mechanism."[70]

**Useful:** "it must be presented in a form matched to the policy decisions to be made, and there ought to be opportunities for follow-up analysis and consultation."[71]

**Timely:** "reports and other work products need to be of use in making decision."[72]

There was general consensus among the meeting attendees that these criteria made OTA valuable to Congress, as did "its effective performance of both a consulting function and a forecasting function to assist congressional staff."[73]

65. GEORGETOWN LAW INST. FOR TECH. LAW & POLICY, IMPROVING TECH EXPERTISE IN CONGRESS: TIME TO REVIVE OTA? 1 (2018).

66. *Id.* (quoting Office of Technology Assessment Act, P.L. 92-484 (1972)).

67. *Id.* at 3.

68. *Id.*

69. *Id.*

70. *Id.*

71. *Id.*

72. *Id.*

73. *Id.* at 16; *see also* ZACH GRAVES & KEVIN KOSAR, BRING IN THE NERDS: REVIVING THE OFFICE OF TECHNOLOGY ASSESSMENT, R ST. 11 (2018), https://www.rstreet.org/wp-content/uploads/2018/04/Final-128-1.pdf ("Maintaining the status quo all but guarantees that suboptimal or outright bad policies will be made more frequently. Failing to augment Congress' technological expertise also ensures the preferences of executive branch agencies and private interests hold the greatest sway in technology policy decisions, to the detriment of the public interest. To address this, Congress needs to bring back its nerds."); Mark Takano, *Let's Revive the Office of Technology Assessment*, MEDIUM (Apr. 17, 2018), https://medium.com/@repmarktakano/lets-revive-the-office-

Although the Georgetown meeting and report focused on technology policy in general, all of this reasoning resonates for cybersecurity. The pace of new threats is ever-increasing, and there is an urgent need for our laws to keep up. Every day, cybersecurity researchers spot new trends in threats from around the globe. To be sure, there is a great deal of valuable cybersecurity expertise in many executive branch agencies, such as the National Security Agency, Department of Homeland Security, and the National Institute of Standards and Technology.[74] As Blair outlined, however, there is tremendous need for internal expertise in Congress to help develop cybersecurity laws that address modern threats. Although some staffers on the relevant committees are knowledgeable about cybersecurity issues, this does not replace a centralized source of expertise from which every member of Congress can draw.

Internal cybersecurity expertise can help Congress replace outdated state and federal laws with statutes that are more effective. Policymakers often conflate the terms "privacy" and "cybersecurity"; while the terms are related, they are distinct.[75] An internal group of experts—whether in the form of OTA or a different organizational structure—would help to inform members of Congress about the current threats and allow them to modernize cybersecurity law.

The challenges that Congress will confront will become ever more complex as technology continues to evolve. Artificial intelligence, quantum computing, and other evolving technologies provide immense potential for innovation, but they also require generalist policymakers to have a deep and meaningful understanding of the inherent cybersecurity issues that accompany them.

It is particularly important for policymakers to have an understanding of the cybersecurity implications of technology at the earliest stages. Such discussions help not only policymakers, but also industry and academia to anticipate challenges and address them before vulnerabilities become baked into the products and services. Indeed, some attribute the security vulnerabilities of the modern Internet to the failure to anticipate the threats that the system would later face.[76]

There may be other ways to inform Congress. A new Article I agency such as OTA may not be politically or economically viable, particularly if the federal

of-technology-assessment-8e5e2631e322 ("Members of Congress bring a great deal of experience and expertise on a number of issues, but we must acknowledge our blind spots. When it comes to the policy challenges presented by new technology—we are not seeing all the relevant issues. With that in mind, I urge you to support funding for the Office of Technology Assessment.").

74. GEORGETOWN LAW INST. FOR TECH. LAW & POLICY, IMPROVING TECH EXPERTISE IN CONGRESS: TIME TO REVIVE OTA? 1 (2018).

75. *See* Anas Baig, *Don't Mix the Two Up: What is the Difference Between Privacy & Security?*, TRIPWIRE (Nov. 7, 2018), https://www.tripwire.com/state-of-security/security-awareness/difference-between-privacy-security/ ("To put it simply, privacy means taking steps to keep your data away from the reach of unauthorized individuals. Security means keeping your data protected against illegal attempts to access or corrupt it.").

76. *See* Craig Timberg, *A Flaw in the Design*, WASH. POST (May 30, 2015), https://www.washingtonpost.com/sf/business/2015/05/30/net-of-insecurity-part-1/?utm_term=.61b611ae9c42 ("Even as scientists spent years developing the Internet, few imagined how popular and essential it would become. Fewer still imagined that eventually it would be available for almost anybody to use, or to misuse.").

budget tightens. Congress might create a new standing committee on cybersecurity, hiring more staff within that committee to lend expertise. Or it might simply call more hearings to hear from subject-area experts rather than industry and interest groups. But attempts to hack cybersecurity law should be guided by the principle that any changes must be as informed as possible. To increase the likelihood that lawmakers are informed, Congress must hear directly from the engineers and scientists who can help them understand how the underlying technology functions. This will allow the lawyers, policymakers, and technologists to work together to attempt to develop policies that improve public and private cybersecurity.

### *B. Clear*

At the heart of many cybersecurity requirements for private companies is "reasonableness." These statutes and regulations rely on the balancing tests that are familiar throughout many areas of law.[77]

Most state data security laws only require "reasonable" security procedures and policies.[78] As cybersecurity attorney Philip N. Yannella wrote in 2018, the "reasonableness" concept in the data security realm "is a notoriously vague standard that often turns on whims of the fact-finder for highly case-specific reasons, making it difficult for a business to draw clear lines."[79] Moreover, Yannella noted, "what constitutes reasonable data security may shift depending on the nature of the data held by the business, the industry, and the scope of the threats," and the concept of reasonableness "for a Fortune 100 technology company may not be the same as for a small or medium sized company."[80] Even a well-inten-

77. *See* Louis Kaplow, *On the Design of Legal Rules: Balancing Versus Structured Decision Procedures*, 132 HARV. L. REV. 992, 993 (2019) ("Balancing is a familiar mode of decisionmaking in the law and beyond. When one consideration favors a particular decision (say, liability) and another opposes it, it seems to be the essence of reason that the superior decision reflects the balance of the competing forces, taking into account the weight of the evidence and the importance of each factor. Many legal rules, such as the negligence test for tort liability, operate in this fashion.").

78. *See, e.g.*, MD. CODE, COM. LAW 14-3503(a) (West 2007) ("To protect personal information from unauthorized access, use, modification, or disclosure, a business that owns or licenses personal information of an individual residing in the State shall implement and maintain reasonable security procedures and practices that are appropriate to the nature of the personal information owned or licensed and the nature and size of the business and its operations."); TEX. BUS. & COM. CODE § 48.102(a) (West 2005) ("A business shall implement and maintain reasonable procedures, including taking any appropriate corrective action, to protect and safeguard from unlawful use or disclosure any sensitive personal information collected or maintained by the business in the regular course of business.").

79. Philip N. Yannella, *What Does "Reasonable" Data Security Mean, Exactly?*, BALLARD SPAHR LLP: CYBERADVISER (July 20, 2018), https://www.cyberadviserblog.com/2018/07/what-does-reasonable-data-security-mean-exactly/; *see also* Alex Bossone, *The Battle Against Breaches: A Call for Modernizing Federal Consumer Data Security Regulation*, 69 FED. COMM. L.J. 227, 238 (2018) ("Based on the somewhat contradictory opinions federal courts have handed down, it is evident that companies are in need of clearer guidance on how to properly secure their data systems, and the consumers could benefit from a more developed statutory framework.").

80. Yannella, *supra* note 79.

tioned company that genuinely wants to comply with the expectations of lawmakers and regulators may be unable to do so, as they are left guessing as to what "reasonableness" means.

This conundrum was at the heart of the *FTC v. LabMD* case, in which the FTC brought a Section 5 unfairness complaint against a medical testing company that the Commission alleged to have engaged "in a number of practices that, taken together, failed to provide reasonable and appropriate security for personal information on its computer networks."[81] The Commission ordered LabMD to develop a data security program that complied with the Commission's "reasonableness" expectations.[82] The U.S. Court of Appeals for the Eleventh Circuit reversed, ruling that the FTC could not require the company "to overhaul and replace its data security program to meet an indeterminable standard of reasonableness."[83] The Eleventh Circuit provided the following hypothetical scenario to demonstrate why such an order is unenforceable. Imagine, the court wrote, that the FTC asked a district court to order the company to show cause why it did not follow the order to have a "reasonably designed" security program."[84]

> The Commission's motion alleges that LabMD's program failed to implement "x" and is therefore not "reasonably designed." The court concludes that the Commission's alleged failure is within the provision's language and orders LabMD to show cause why it should not be held in contempt.
>
> At the show cause hearing, LabMD calls an expert who testifies that the data-security program LabMD implemented complies with the injunctive provision at issue. The expert testifies that "x" is not a necessary component of a reasonably designed data-security program. The Commission, in response, calls an expert who disagrees. At this point, the district court undertakes to determine which of the two equally qualified experts correctly read the injunctive provision. Nothing in the provision, however, indicates which expert is correct. The provision contains no mention of "x" and is devoid of any meaningful standard informing the court of what constitutes a "reasonably designed" data-security program. The court therefore has no choice but to conclude that the Commission has not proven—and indeed cannot prove—LabMD's alleged violation by clear and convincing evidence.
>
> If the court held otherwise and ordered LabMD to implement "x," the court would have effectively modified the injunction at a show cause hearing. This would open the door to future modifications, all improperly made at show cause hearings. Pretend that LabMD implemented "x" pursuant to the court's order, but the FTC, which is continually monitoring LabMD's compliance with the court's injunction, finds that "x" failed to bring the system up to the FTC's conception of reasonableness. So, the FTC again moves the district court for an order to show cause. This time, its motion

81. LabMD, Inc. v. Fed. Trade Comm'n, 894 F.3d 1221, 1225 (11th Cir. 2018).
82. *Id.* at 1236.
83. *Id.*
84. *Id.*

> alleges that LabMD failed to implement "y," another item the Commission thinks necessary to any reasonable data-security program. Does the court side with the Commission, modify the injunction, and order the implementation of "y"? Suppose "y" fails. Does another show cause hearing result in a third modification requiring the implementation of "z"?
>
> The practical effect of repeatedly modifying the injunction at show cause hearings is that the district court is put in the position of managing LabMD's business in accordance with the Commission's wishes. It would be as if the Commission was LabMD's chief executive officer and the court was its operating officer. It is self-evident that this micromanaging is beyond the scope of court oversight contemplated by injunction law.[85]

The Eleventh Circuit offered this example to demonstrate that just as a court order with such a vague standard would be unreasonable, so too should be an FTC order that requires an unspecified level of "reasonableness."[86] One expert's legitimate idea of "reasonableness" could be entirely unreasonable to another, even if both are acting in good faith to attempt to increase the security of a system, network, or data.[87]

As Gus Hurwitz wrote, the Eleventh Circuit's reasoning extends not only to whether an FTC order is enforceable by a court, but whether FTC-regulated companies could comply with a vague standard:

> Most businesses are no more expert in data security than a typical judge. Indeed, courts are assisted by expert witnesses and extensive briefing on the specific issues before them. If the standard proffered by the FTC is too indeterminate for a court to objectively evaluate conduct in specific cases, then clearly it is too indeterminate to be applied in the general case.[88]

Debates regarding the need for clarity and specificity in legal requirements existed long before cybersecurity.[89] In 1964, George C. Christie argued that

85. *Id.* at 1236–37.

86. *Id.*

87. *See* Robert Cattanach & Sam Bolstad, *FTC's Data Security Authority Curbed by 11th Circuit*, DORSEY & WHITNEY (June 7, 2018), https://www.dorsey.com/newsresources/publications/client-alerts/2018/06/ftcs-data-security-authority ("The LabMD opinion provides companies with at least some opportunity to challenge FTC overreach. Companies will still be expected to manage data efficiently, independently, and responsibly, but will now have some foundation to challenge aspirational, vague standards asserted in ongoing enforcement actions or negotiations with the FTC, and try to limit the FTC's enforcement action to specifically identified data security deficiencies."); Marcie Ernst, *4 Questions You Need to Ask About FTC Enforcement Actions on Data Privacy Violations*, TRUST THE LEADERS: FTC ENFORCEMENT ACTIONS, Winter 2019, at 21, https://www.sgrlaw.com/wp-content/uploads/2019/02/FTC-Enforcement-Actions.pdf ("Under the Eleventh Circuit's decision in *LabMD*, specific benchmarks for data security, rather than vague standards of 'reasonableness,' will be required for companies accused of failing to safeguard data.").

88. Justin (Gus) Hurwitz, *Response to McGeveran's* The Duty of Data Security: *Not the Objective Duty He Wants, Maybe the Subjective Duty We Need*, 103 MINN. L. REV. HEADNOTES 139, 145 (2019).

89. *See* Jason Scott Johnston, *Uncertainty Chaos and the Torts Process: An Economic Analysis of Legal Form*, 76 CORNELL L. REV. 341, 344–45 (1991) ("Members of the Critical Legal Studies ('CLS') movement have argued that all legal doctrine must be indeterminate and unpredictable to some degree, and that the debate over legal formality and predictability should not be allowed to obscure the inevitability of choice in adjudication. For commentators on the other side of the political/economic spectrum, by contrast, the problem is not that all law is indeterminate, but merely that balancing tests do not properly constrain legal decisionmakers and do not adequately delineate private property and the sphere of individual autonomy."); James G. Wilson, *Surveying the Forms of Doctrine on the Bright Line-Balancing Test Continuum*, 27 ARIZ. ST. L.J. 773, 773 (1995) ("The long-

vagueness is "an inescapable aspect of our language," and that it has "given our law a much needed flexibility."[90] Pierre Schlag, in contrast, wrote in 1985 that rules—rather than standards—"draw a sharp line between forbidden and permissible conduct, allowing persons subject to the rule to determine whether their actual or contemplated conduct lies on one side of the line or the other," and that this "sharp line also assures that no desirable or permissible conduct will be chilled."[91] On the other hand, Schlag noted, rules "permit and encourage activity up to the boundary of permissible conduct," while more flexible standards "allow the addressees to make individualized judgments about the substantive offensiveness or nonoffensiveness of their own actual or contemplated conduct."[92]

Cybersecurity law must strike a better balance on the continuum of rules and standards. As I describe in the next Section, cybersecurity laws must be adaptable to new technologies and industry standards for data security. Companies, however, must have some current guidance as to what would satisfy these requirements. Although "reasonableness" is a laudable concept and adequate starting point for discussion, it is not sufficient for a cybersecurity law to merely require a company to provide "reasonable" data security protections without providing further direction. As the Eleventh Circuit aptly explained in its *LabMD* opinion, such a broad directive does not provide companies with sufficient certainty that they are compliant.[93] Cybersecurity requires companies to develop detailed policies and procedures, and to train new and current employees. Before a company invests the time and money in developing these new policies and procedures, it should have some clarity regarding the applicable regulatory requirements.

Cybersecurity also requires significant investments in software and hardware upgrades and replacements. It is rare to find a company with an unlimited information technology budget;[94] an information security director could better make the case for new investments in technology by demonstrating that these investments would satisfy current regulatory requirements. If that manager were to merely say, "it might help but we don't know, because the law only requires 'reasonable' security," then the executive suite would probably be less inclined to approve the investment.

standing jurisprudential controversy over whether courts should utilize bright line rules or balancing tests has failed to inform sufficiently lawyers and judges. For many years, most analysts contrasted rigid rules, such as the United States Supreme Court's striking down all legislative vetoes in *I.N.S. v. Chadha*, with conclusory standards, like *Morrison v. Olson*'s upholding special prosecutors because they did not 'impermissibly undermine the powers of the Executive Branch.") (footnote omitted).

90. George C. Christie, *Vagueness and Legal Language*, 48 MINN. L. REV. 885, 911 (1964).

91. *See* Pierre Schlag, *Rules and Standards*, 33 UCLA L. REV. 379, 384 (1985).

92. *Id.* at 384–85.

93. LabMD v. Fed. Trade Comm'n, 894 F.3d 1221, 1235 (11th Cir. 2018).

94. *See* Steve Morgan, *Survey: 87 Percent of IT Leaders Say They Need Up to 50 Percent More Cybersecurity Budget*, CYBERCRIME MAG. (Apr. 16, 2018), https://cybersecurityventures.com/ey-global-information-security-survey-2017-18/ ("One statistic that really grabbed our attention is that 87 percent of respondents to an EY survey say they need up to 50 percent more cybersecurity budget. With cybercrime at an all-time high, that's as scary as the cyber threats are.").

To be sure, I am not arguing against any flexibility in cybersecurity law. Cybersecurity incidents are inherently fact-intensive, and the law must have sufficient breathing space to account for the many types of threats and responses that can arise from an incident. The regulatory requirements, however, must strike a better balance between "reasonableness standards" and specific requirements, and, currently, the law is too skewed toward reasonableness. While a number of different combinations of safeguards, when considered as a whole, might be considered reasonable, companies should at least have a concrete understanding of some types of precautions that would satisfy this standard.

Ohio's state legislature attempted to address this problem in an innovative manner in its 2018 Data Protection Act.[95] The statute provides companies with an affirmative defense in tort claims arising from data breaches if they conform with a particular data security standard, such as the NIST Cybersecurity Framework or the FedRAMP security assessment framework.[96] Companies are still subject to the "reasonableness" requirements of state data security regulations and common law tort claims such as negligence.[97] But they now have some level of assurance (though far from absolute, as it is only an affirmative defense) that complying with a specified cybersecurity framework or standard will meet that reasonableness requirement.[98] This increases the likelihood that a company will invest in compliance with those standards. The Ohio model strikes a better balance between the need for flexible and adjustable standards with companies' desire to have confidence that their investments will comply with the expectations of courts and regulators.

In short, rational companies likely *want* to comply with regulators' expectations for cybersecurity. Not only do the companies have an interest in avoiding the fines, legal fees, and negative publicity associated with enforcement actions and litigation, but it is in their best interests to enact strong cybersecurity safeguards. Such protections also reduce the possibility that businesses will lose confidential trade secrets or suffer the costly disruption of ransomware attacks. The primary challenge is that businesses do not have sufficient certainty as to precisely *what* those regulatory standards are. The requirements are dispersed across numerous state and federal statutes and regulations, and they often only impose vague reasonableness standards.[99] Any hack of the cybersecurity legal system should attempt to provide at least a bit more clarity to companies to allow them to be more certain in their cybersecurity investments.

95. OHIO REV. CODE ANN. §§ 1354.01–05 (LexisNexis 2019).

96. *Id.* § 1354.03.

97. Yannella, *supra* note 79.

98. To be sure, the Ohio law has attracted some criticism for its reliance on broad frameworks that might not provide the certainty that Ohio seeks. *See* Jason Wool, *Cybersecurity Lawmaking Needs Help from Specialists*, LAW360 (June 4, 2019, 1:50 PM), https://www.law360.com/articles/1164968/cybersecurity-lawmaking-needs-help-from-specialists ("[T]he frameworks named in the statute make little sense in practice as applied to most companies. For instance, a company can choose to conform its program to the National Institute of Standards and Technology's Cybersecurity Framework, which NIST has repeatedly resisted categorizing as a standard as opposed to a risk management tool explicitly designed to be flexible and nonprescriptive.").

99. *See Data Security Laws | Private Sector*, *supra* note 12.

### *C. Adaptive*

Cybersecurity law should be capable of changing at the same pace as cybersecurity threats and defensive measures. Therefore, if a legal rule (such as a statute) is incapable of being adjusted frequently due to constraints such as the political difficulty of enacting new legislation, then it is understandable to avoid codifying a particular technological requirement that currently is state-of-the-art, but may well be antiquated within a few years.

For instance, until around 2017, cybersecurity experts largely advocated for complex and long passwords that must be changed frequently. But recently, guidance has focused less on password complexity and change frequency, and more on ensuring that the passwords are not on lists of commonly used terms.[100]

As discussed in the previous Section, cybersecurity law should be specific enough to identify the areas—such as password length—that companies must comply with. But it must be flexible enough to adjust to new developments in the law.

It is not realistic to expect statutes to sufficiently adapt to the constant changes in cybersecurity demands. Congress can take years to agree on the final text of laws, and final passage often is subject to political whims that may be entirely unrelated to cybersecurity, such as horsetrading for other legislation. By the time lawmakers settle on final language, new cybersecurity challenges may have emerged. Due to the difficulty of passing statutes, it is unrealistic to expect them to explicitly address particular technology or safeguards.[101]

To address this problem, Congress should enact a general data security and breach notification statute and delegate rulemaking authority to an expert agency. That agency would have rulemaking authority to enact specific requirements. Although the rulemaking process can be lengthy—particularly with the inevitable court challenges to the final rules—it likely would be more efficient and adaptive than relying on Congress to pass a new law.

There is some precedent for this model. The Gramm-Leach-Bliley Act, a 1999 overhaul of the U.S. financial regulatory system, contains a "Safeguards Rule," which broadly requires financial institutions to adopt data security safeguards that "insure the security and confidentiality of customer records and information," "protect against any anticipated threats or hazards to the security or integrity of such records," and "protect against unauthorized access to or use of such records or information that could result in substantial harm or inconvenience to any customer."[102] The statute delegates regulatory authority to financial

100. Sandra Henry-Stocker, *Dealing with NIST's About-Face on Password Complexity*, NETWORKWORLD (June 5, 2017, 11:13 AM), https://www.networkworld.com/article/3199607/dealing-with-nists-about-face-on-password-complexity.html.

101. *See* Michael Kirby, *The Fundamental Problem of Regulating Technology*, 5 INDIAN J.L. & TECH. 1, 24 (2009) ("In the face of radically changing technologies and the danger of a growing democratic deficit, it will obviously be necessary to adapt and supplement the lawmaking processes we have hitherto followed in most countries. Various forms of delegated legislation may need to be considered. So may the enactment of overarching laws, expressed in general terms, which will not be quickly reduced to irrelevancy by further technological change.").

102. 15 U.S.C. § 6801(b) (2018).

regulatory agencies, such as the Federal Trade Commission and Office of Comptroller of the Currency.[103] This structure not only allows agencies to update the regulations to address current threats, but it also enables them to customize their regulations to the cybersecurity challenges that confront their particular industries.[104]

Similarly, in 1998, Congress passed the Children's Online Privacy Protection Act ("COPPA"), which restricts websites' collection of personal information from children who are under thirteen years old.[105] The statute broadly delegates to the FTC the duties to, among other things, "require the operator of any website or online service directed to children that collects personal information from children or the operator of a website or online service that has actual knowledge that it is collecting personal information from a child" and "prohibit conditioning a child's participation in a game, the offering of a prize, or another activity on the child disclosing more personal information than is reasonably necessary to participate in such activity."[106] In late 2012, the FTC overhauled its COPPA regulations to account for changes in technology.[107] For instance, it added geolocation data and persistent identifiers to its list of information covered by the regulation, and it clarified that the regulation applies to advertising networks that collect personal information.[108]

The GLBA and COPPA model—setting broad standards in statute while delegating particular requirements to an expert agency—would be well-suited for general data security requirements.[109] The FTC would be the best suited to promulgate these regulations, as it already brings data security actions under Section 5 of the FTC Act.[110] If Congress were to pass legislation that provides the Commission with explicit rulemaking authority, the FTC could more agilely

103. *Id.*

104. *See* FTC Seeks Comment on Proposed Amendments to Safeguards and Privacy Rules, FED. TRADE COMM'N (Mar. 5, 2019), https://www.ftc.gov/news-events/press-releases/2019/03/ftc-seeks-comment-proposed-amendments-safeguards-privacy-rules ("'We are proposing to amend our data security rules for financial institutions to better protect consumers and provide more certainty for business,' said Andrew Smith, Director of the FTC's Bureau of Consumer Protection. 'While our original groundbreaking Safeguards Rule from 2003 has served consumers well, the proposed changes are informed by the FTC's almost 20 years of enforcement experience.'").

105. 15 U.S.C. § 6502 (2018).

106. *Id.*

107. FTC's Revised COPPA Rule: Five Need-to-Know Changes for Your Business, FED. TRADE COMM'N (Dec. 19, 2012, 12:01 PM), https://www.ftc.gov/news-events/blogs/business-blog/2012/12/ftcs-revised-coppa-rule-five-need-know-changes-your-business.

108. *Id.*

109. *See* CONSUMER FED'N OF AMERICA, COMMENTS OF THE CONSUMER FEDERATION OF AMERICA TO THE FEDERAL TRADE COMMISSION: COMPETITION AND CONSUMER PROTECTION IN THE 21ST CENTURY HEARINGS 2 (2018), https://consumerfed.org/wp-content/uploads/2018/08/cfa-comments-regarding-ftc-remedial-authority-to-deter-unfair-deceptive-conduct.pdf [hereinafter *Comments*] ("[M]any of the FTC rules that we rely on the protect consumers, such as those concerning children's online privacy and telemarking abuses, have been promulgated at the direction of Congress. These rules are issued to implement the underlying statutes, which typically set out the public policy objectives at a high level. They describe in more granular detail which entities are covered and under what circumstances, and what is expected of them. FTC rules help businesses and consumers understand their rights and responsibilities.").

110. *See id.*

adopt specific regulatory requirements to current technological needs. In fact, both Republican and Democratic FTC commissioners have long called for Congress to provide it with explicit data security rulemaking authority.[111]

More concrete regulations from an expert agency also would address the need for clarity described in the previous Section. Currently, to determine the FTC's data security expectations, companies must read the tea leaves based on the dozens of data security enforcement actions that the Commission has brought against companies after breaches under Section 5 of the FTC Act.[112] These cases are fact-specific, and often only provide a high-level overview of the data security failures that led to the enforcement action.[113] Although the FTC has attempted to synthesize the lessons from these cases in a 2015 guide[114] and follow-up blog posts,[115] the guide and blog posts do not provide the same level of clarity and specificity as binding regulations. Nor can the blog posts or other informal guidance sufficiently adapt to technological changes; they are based on the cases that the FTC has brought over the past two decades. Many of these cases deal with old technologies and compromises, such as SQL injection attacks, which may not be as immediately applicable to the most pressing current threats.[116]

A benefit of the rulemaking process is that it allows the public to participate through the notice-and-comment process.[117] This allows consumer groups and privacy advocates to inform the agency of the greatest threats and cybersecurity shortcomings of companies, and it allows industry to weigh in on the solutions that they have found to be effective and realistic. It also allows neutral experts—such as academics—to provide insight into the safeguards that they believe would be best to address the problem.

To be clear, data security rulemaking authority would not result in constant changes to data security requirements. The notice-and-comment process can take years between the initial notice of proposed rulemaking and the final rule,[118] as the FTC would review comments and address them as it crafts final rules. And a

111. *See* FED. TRADE COMM'N, PREPARED STATEMENT OF THE FEDERAL TRADE COMMISSION: OVERSIGHT OF THE FEDERAL TRADE COMMISSION BEFORE THE COMMITTEE ON COMMERCE, SCIENCE, AND TRANSPORTATION, SUBCOMMITTEE ON CONSUMER PROTECTION, PRODUCT SAFETY, INSURANCE, AND DATA SECURITY UNITED STATES SENATE 7 (Nov. 27, 2018) ("[T]he FTC lacks broad APA rulemaking authority for data security generally. The Commission continues to reiterate its longstanding bipartisan call for comprehensive data security legislation.").

112. *See Comments*, *supra* note 109, at 4.

113. *See id.* at 2.

114. FED. TRADE COMM'N, START WITH SECURITY: A GUIDE FOR BUSINESS (2015).

115. *See Stick with Security: A Business Blog Series*, FED. TRADE COMM'N (Oct. 2017), https://www.ftc.gov/tips-advice/business-center/guidance/stick-security-business-blog-series.

116. FED. TRADE COMM'N, *supra* note 114, at 10.

117. *See* Donald J. Kochan, *The Commenting Power: Agency Accountability Through Public Participation*, 70 OKLA. L. REV. 601, 602 (2018) ("The commenting power ensures that the ballot box is not the only place where citizens get to serve a checking function on government; they have it also in their ability to participate in agency rulemaking. Professor and former United States Deputy Chief Technology Officer Beth Simone Noveck summarized it well when she explained, 'Participation in rulemaking is one of the most fundamental, important, and far-reaching of democratic rights.' Rather than lying in another branch of government, as do most of what we consider checks and balances, the commenting power rests in the people.").

118. *See A Guide to the Rulemaking Process*, OFFICE OF THE FED. REGISTER, https://www.federalregister.gov/uploads/2011/01/the_rulemaking_process.pdf (last visited Mar. 23, 2020).

party may well challenge those rules in court. This "ossification" allows what Aaron L. Nielson calls "sticky regulations," which he defines as "rules that cannot be changed or rescinded quickly."[119] Because agencies inevitably face some degree of delay, he writes, they can "better regulate into the future."[120]

By delegating cybersecurity rulemaking authority to the FTC (or another expert agency), Congress would allow the promulgation of regulations that adapt to new technology, but also would be sufficiently sticky so as to provide companies with some certainty that they won't be quickly rescinded. To the extent that the FTC promulgated new regulations every few years, these regulations would not necessarily be a radical overhaul of its previous expectations; rather they could provide modest updates to incorporate the current industry standards for safeguards. In between formal updates of the new regulations, the FTC could issue guidance which, while nonbinding, could provide companies with some assurance that their actions meet the expectations of regulators.

### *D. Comprehensive*

Cybersecurity laws must comprehensively address the full range of threats that the United States faces in cyberspace. Unfortunately, U.S. laws are narrowly focused on a subset of older cybersecurity threats, such as data breaches.[121] While these threats to the confidentiality of personal information remain significant concerns, they do not encompass the full range of challenges that we *currently* confront.

To understand the myopic nature of U.S. cybersecurity law, it is useful to examine the scope of the work that cybersecurity professionals conduct on a day-to-day basis. Cybersecurity is commonly conceived as the "CIA Triad," standing for confidentiality, integrity, and availability.[122] Confidentiality "involves access to data by individuals or entities that the owner of the data does not intend."[123]

119. Aaron L. Nielson, *Sticky Regulations*, 85 U. CHI. L. REV. 85, 90 (2018).

120. *Id.* at 142–43 ("If agencies could immediately change the rules, regulated parties would be much less willing to accept what agencies say. And for that reason, regulated parties would be much less willing to trust incentives. To the extent that uncertainty discourages the sort of innovation that the agency prefers, it narrows an agency's long-term options. So to the extent that ossification reduces uncertainty, it expands an agency's options.").

121. Kristen E. Eichensehr, *Giving Up on Cybersecurity*, 64 UCLA L. REV. DISCOURSE 320, 337 (2016).

122. *Id.* at 324.

123. *Id.*

A typical threat to confidentiality would include a data breach.[124] Confidentiality attacks include compromises of personal information,[125] classified government information,[126] and corporate trade secrets.[127]

Threats to integrity "involve unauthorized changes to data" and "are particularly troubling because they are difficult to detect and once any integrity problem is discovered, it tends to cast doubt on the accuracy and reliability of all the other data on the system."[128] In 2013, for instance, the Syrian Electronic Army hacked the Associated Press Twitter account and sent the following message to almost 2 million people: "Breaking: Two Explosions in the White House and Barack Obama is injured."[129] Although the Associated Press quickly corrected the fake tweet, it caused the Dow Jones Industrial Average to plunge nearly 150 points within minutes.[130] Imagine other integrity attacks that could cause even more damage, such as the hack of an emergency alert system that falsely reports a nuclear attack in a major city, causing mass chaos as people attempt to evacuate. Or imagine an integrity attack on industrial control systems of a large manufacturing plant, causing equipment malfunctions and potentially injury to factory workers.

Threats to availability "occur when data or systems are not accessible to authorized users when they are supposed to be."[131] An increasingly common availability attack is ransomware, in which a program encrypts data on a computer or system, and the victim can only access the data by paying ransom to the

124. *Types of Data Breaches*, WHITE HAT SECURITY, https://www.whitehatsec.com/glossary/content/types-data-breaches (last visited Mar. 23, 2020).

125. *See, e.g.*, Allen St. John, *The Data Breach Next Door*, CONSUMER REP. (Jan. 31, 2019), https://www.consumerreports.org/data-theft/the-data-breach-next-door/ ("Once their personal data is stolen, consumers are more vulnerable to crimes such as identity theft and spear-phishing emails that can trick even cautious people into revealing credit card and Social Security numbers, along with log-in credentials for social media or bank accounts.").

126. *See, e.g.*, Richard Esposito & Matthew Cole, *How Snowden Did It*, NBC NEWS (Aug. 26, 2013, 10:59 AM), https://www.nbcnews.com/news/world/how-snowden-did-it-flna8C11003160 ("When Edward Snowden stole the crown jewels of the National Security Agency, he didn't need to use any sophisticated devices or software or go around any computer firewall. All he needed, said multiple intelligence community sources, was a few thumb drives and the willingness to exploit a gaping hole in an antiquated security system to rummage at will through the NSA's servers and take 20,000 documents without leaving a trace.").

127. *See, e.g.*, Jonathan Landay, *U.S. Initiative Warns Firms of Hacking by China, Other Countries*, REUTERS (Jan. 7, 2019, 9:49 AM), https://www.reuters.com/article/us-usa-cyber-china/u-s-initiative-warns-firms-of-hacking-by-china-other-countries-idUSKCN1P11K5 ("U.S. companies hit by recent attacks included Hewlett Packard Enterprise Co and International Business Machines Corp. IBM said it had no evidence that sensitive corporate data had been compromised. Hewlett Packard Enterprise has said the security of HPE customer data is a 'top priority.'").

128. Eichensehr, *supra* note 121, at 325.

129. Max Fisher, *Syrian Hackers Claim AP Hack That Tipped Stock Market by $136 Billion. Is It Terrorism?*, WASH. POST (Apr. 23, 2013, 3:31 PM), https://www.washingtonpost.com/news/worldviews/wp/2013/04/23/syrian-hackers-claim-ap-hack-that-tipped-stock-market-by-136-billion-is-it-terrorism/.

130. *Id.*

131. Eichensehr, *supra* note 121, at 325 ("For example, in 2012 and early 2013, distributed denial of service (DDoS) attacks rendered the websites of numerous U.S. financial institutions inaccessible by flooding them with traffic and thereby preventing legitimate customers from accessing their accounts.").

attacker.[132] The effects can be sweeping. For instance, in 2018, the city of Atlanta spent about $2.6 million to fix problems caused by a ransomware attack that demanded $52,000.[133] In some cases, they still cannot access the data even after paying the ransom.[134] Such attacks can have immediate and devastating consequences. For instance, after two Ohio hospitals were victims of ransomware attacks in November 2018, they were forced to send emergency patients to other hospitals.[135]

In short, policymakers should be concerned about threats to confidentiality, integrity, *and* availability. Unfortunately, U.S. cybersecurity laws primarily focus on protecting confidentiality, and, to a lesser extent, availability.[136]

For instance, the state breach notification laws typically are triggered by the unauthorized acquisition of certain types of personal information,[137] which at its core is related to the confidentiality of data. To be sure, some state breach notice laws mention the goals of "integrity" and "security" in addition to confidentiality.[138] Almost all of them, however, are triggered by an "acquisition" of personal data, meaning that breaches of confidentiality generally are necessary

132. *See generally* Amin Kharraz et al., *Protecting Against Ransomware: A New Line of Research or Restating Classic Ideas?*, 16 IEEE SECURITY & PRIVACY 103, 103 (2018) ("Ransomware is a type of extortion-based attack that locks the victim's digital resources and requests money to release them. The recent resurgence of high-profile ransomware attacks, particularly in critical sectors such as the healthcare industry, has highlighted the pressing need for effective defenses.").

133. *See* Lily Hay Newman, *Atlanta Spent $2.6M to Recover From a $52,000 Ransomware Scare*, WIRED (Apr. 23, 2018, 8:55 PM), https://www.wired.com/story/atlanta-spent-26m-recover-from-ransomware-scare/ ("The Atlanta Department of Procurement lists eight emergency contracts initiated between Match 22 [sic] and April 2 with a total value of $2,667,328. The bulk of the expenditures relate to incident response and digital forensics, extra staffing, and Microsoft Cloud infrastructure expertise, presumably all related to clawing back the systems that the hackers had frozen. The city also spent $50,000 on crisis communications services from the firm Edelman, and $600,000 on incident response consulting from Ernst & Young.").

134. *See* Andy Greenberg, *The Untold Story of NotPetya, The Most Devastating Cyberattack in History*, WIRED (Aug. 22, 2018, 5:00 AM), https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/ ("NotPetya took its name from its resemblance to the ransomware Petya, a piece of criminal code that surfaced in early 2016 and extorted victims to pay for a key to unlock their files. But NotPetya's ransom messages were only a ruse: The malware's goal was purely destructive. It irreversibly encrypted computers' master boot records, the deep-seated part of a machine that tells it where to find its own operating system. Any ransom payment that victims tried to make was futile. No key even existed to reorder the scrambled noise of their computer's contents.").

135. *See* Jessica Davis, *Ohio Hospitals Disrupted by Ransomware Attack*, SECURITY TODAY (Nov. 29, 2018), https://securitytoday.com/articles/2018/11/29/ohio-hospitals-disrupted-by-ransomware-attack.aspx ("The hospitals' IT team took some computer systems offline during the attack to protect patient health data. The hospitals were unable to take care of emergency squad patients, but clinical operations in other units and care settings proceeded as usual.").

136. *See* JAMES R. CLAPPER, STATEMENT FOR THE RECORD: WORLDWIDE CYBER THREATS 5 (2015), https://www.dni.gov/files/documents/HPSCI%2010%20Sept%20Cyber%20Hearing%20SFR.pdf (publishing the statement of James R. Clapper, Director of National Intelligence, before the House Permanent Select Committee on Intelligence) ("Most of the public discussion regarding cyber threats has focused on the confidentiality and availability of information . . . .").

137. *See, e.g.*, CAL. CIV. CODE § 1798.82(g) (West 2017) (defining "breach of the security of the system" as "unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information").

138. *See, e.g.*, IOWA CODE ANN. § 715C.1 (West 2018) (defining "breach of security" as "unauthorized acquisition of personal information maintained in computerized form by a person that compromises the security, confidentiality, or integrity of personal information").

to trigger coverage.[139] Moreover, the breach notice laws cover only the narrow categories of personal information that largely remain tied to the potential for identity theft or other financial harm.[140]

If a hacker were, for instance, to deploy a ransomware attack that rendered files inaccessible to the target company, the company likely would not be obliged to warn consumers or assist them with alternative arrangements.[141] Likewise, some data security laws focus primarily on protecting the confidentiality of information by requiring companies to adopt reasonable procedures to prevent unauthorized parties from acquiring the data.[142] Other state data security laws may at least impose minimal requirements to protect the integrity and availability of data.[143] For instance, California's data security law more broadly provides that "[a] business that owns, licenses, or maintains personal information about a California resident shall implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use, modification, or disclosure."[144] Although the law addresses not only unauthorized access, disclosure, and use, but also destruction and modification, it is at least intended to go beyond confidentiality. Unfortunately, the limited scope of the law's definition of "personal information,"[145] coupled with a broad and vague reasonableness requirement, does little to address the very real integrity and availability threats such as

139. BAKERHOSTETLER, STATE DATA BREACH LAW SUMMARY (2018), https://www.bakerlaw.com/files/Uploads/Documents/Data%20Breach%20documents/State_Data_Breach_Statute_Form.pdf.

140. Ross Kerber, *Hannaford Case Exposes Holes in Law, Some Say 'Identity Theft' Criteria Called Too Narrow*, BOS. GLOBE (Mar. 30, 2018), http://archive.boston.com/business/articles/2008/03/30/hannaford_case_exposes_holes_in_law_some_say/?page=full.

141. *Ransomware Attacks: When Is Notification Required?*, LATHAM & WATKINS (Apr. 26, 2017), https://www.lw.com/thoughtLeadership/LW-ransomware-attacks-when-is-notification-required ("In the absence of any explicit guidance to the contrary by state authorities, application of the ordinary concepts of acquisition and likelihood of harm should mean that, where an attacker merely encrypts (locks up) data containing PII, and forensic analysis reliably indicates that the data has not been viewed, copied, or moved by the attacker, notification should not be required."). In 2018, North Carolina Attorney General Josh Stein recognized this gap in the law and proposed an amendment to North Carolina's breach notice law that would require businesses to notify affected individuals about ransomware attacks. *See* Bradley Barth, *North Carolina Introduces Data Breach Legislation, After Incidents Rise in 2017*, SC MAGAZINE (Jan. 9, 2018), https://www.scmagazine.com/home/security-news/government-and-defense/north-carolina-introduces-data-breach-legislation-after-incidents-rise-in-2017/.

142. *See, e.g.*, FLA. STAT. § 501.171(2) (West 2019) ("Each covered entity, governmental entity, or third-party agent shall take reasonable measures to protect and secure data in electronic form containing personal information."); UTAH CODE § 13-44-S201(1) (West 2019) ("Any person who conducts business in the state and maintains personal information shall implement and maintain reasonable procedures to . . . prevent unlawful use or disclosure of personal information collected or maintained in the regular course of business.").

143. *See Defining Cybersecurity Law*, *supra* note 8, at 1013.

144. CAL. CIV. CODE ANN. § 1798.81.5(b) (West 2016).

145. The California Civil Code defines "personal information as:

> An individual's first name or first initial and his or her last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted or redacted:
> (i) Social security number.
> (ii) Driver's license number or California identification card number.
> (iii) Account number, credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account.
> (iv) Medical information.
> (v) Health insurance information.

ransomware and website defacement, which often involve other forms of data such as corporate trade secrets, public-facing websites, and personal information that does not relate to financial harm or identity theft.

To be sure, confidentiality-focused safeguards may help to promote integrity and availability. For instance, if a state were to require multifactor authentication in an effort to reduce the likelihood that an unauthorized party would acquire customers' personal information, that requirement also could reduce the chances that a hacker would alter data on the system or render it unavailable. Regulating confidentiality, however, may not necessarily address all threats to integrity and availability. For instance, consider a technological control that could reduce the spread of ransomware throughout a system. If a regulation was aimed at merely safeguarding the confidentiality of personal information, it likely would not require that safeguard. From the outset, laws should aim to protect all three prongs of the CIA Triad.[146]

The CFAA[147] and EEA[148] focus not only on confidentiality, but also integrity and availability to some extent. This is some progress, though the laws are typically enforced after the fact against hackers, and do little to encourage the *companies* to enact safeguards that promote the full scope of the CIA Triad.[149] And because the EEA is focused on trade secrets, the prosecutions and civil cases brought under the statute overwhelmingly focus on *theft* rather than alterations.[150]

I do not intend to suggest that cybersecurity law should no longer protect confidentiality. To the contrary, some of our greatest cybersecurity compromises in recent years, such as the hacking of John Podesta's email and the Democratic National Committee,[151] have involved breaches of confidentiality. But the

(B) A username or email address in combination with a password or security question and answer that would permit access to an online account.

*Id.*

146. *See Defining Cybersecurity Law*, *supra* note 8, at 998–99 ("To be sure, we want to make sure that cybersecurity law attempts to prevent breaches of confidentiality that invade individual privacy and exposes corporate intellectual property and other sensitive information. However, cybersecurity law should not focus on confidentiality to the exclusion of integrity and availability. A comprehensive approach to cybersecurity law will consider all three prongs of the CIA Triad.").

147. *See* 18 U.S.C. § 1030(a)(5)(A) (2018) (creating a criminal penalty for an individual who "knowingly causes the transmission of a program, information, code, or command, and as a result of such conduct, intentionally causes damage without authorization, to a protected computer"); 18 U.S.C. § 1030(a)(7)(C) (2018) (creating a criminal penalty for an individual who "with intent to extort from any person any money or other thing of value, transmits in interstate or foreign commerce any communication containing any . . . demand or request for money or other thing of value in relation to damage to a protected computer, where such damage was caused to facilitate the extortion").

148. 18 U.S.C. § 1831(a)(2) (2018) (creating a criminal penalty for an individual who knowingly, in certain circumstances, "without authorization copies, duplicates, sketches, draws, photographs, downloads, uploads, alters, destroys, photocopies, replicates, transmits, delivers, sends, mails, communicates, or conveys a trade secret").

149. *Defining Cybersecurity Law*, *supra* note 8, at 998–99.

150. *Id.* at 1019–20.

151. *See* Jon Swaine & Andrew Roth, *U.S. Indicts 12 Russians for Hacking DNC Emails During the 2016 Election*, GUARDIAN (July 13, 2018, 9:29 PM), https://www.theguardian.com/us-news/2018/jul/13/russia-indictments-latest-news-hacking-dnc-charges-trump-department-justice-rod-rosenstein.

law should not focus solely on confidentiality to the exclusion of integrity and availability.

Moreover, policymakers should strive to protect against a broader range of harms. Cybersecurity law has focused largely on preventing and remediating financial harms;[152] data security and breach notification laws provide the greatest protection to data whose breach could lead to financial fraud or identity theft, and computer hacking laws are in part defined by the scope of the financial harms that the perpetrators cause. To be sure, cybersecurity law should seek to prevent these harms. But data breaches cause far more than just financial harm. A breach of personal information can upend an individual's personal life. For instance, in 2015, hackers published membership lists for Ashley Madison, a website that matched people who were searching for extramarital affairs.[153] As Daniel Solove and Danielle Citron aptly demonstrated, this breach caused anxiety that reached far beyond financial harm:

> The hackers stole information related to users' sexual desires and personally identifying information and posted it online. The knowledge that employers, family, and friends might discover one's intimate desires and fantasies produced significant anxiety. Ashley Madison users who were active members of the military worried that they might face penalties because adultery is a punishable offense under the Army's Military Code of Conduct. Following the breach, several affected individuals committed suicide.[154]

A narrow focus on economic harm would do little to prevent or remediate future attacks. While some information may not at first blush appear to be terribly "personal," it could cause great harm to an individual if disclosed. U.S. cybersecurity laws must move beyond their myopic focus on financial harms caused by data breaches and address the many vectors of cyberattacks that can harm individuals.[155]

Likewise, cybersecurity law must better address harms to national security. For instance, there is little dispute that Russia's hacking of the Democratic National Committee and Clinton Campaign Chairman John Podesta was caused in part by cybersecurity failures.[156] Policymakers, however, also should view Russia's use of fake social media content during the 2016 election as a cybersecurity problem. Russia's persistent dissemination of falsehoods via U.S. social media services threatened the integrity of information that was central to the U.S. democratic system.

---

152. *Defining Cybersecurity Law*, *supra* note 8, at 1008.

153. *See* Kim Zetter, *Hackers Finally Post Stolen Ashley Madison Data*, WIRED (Aug. 18, 2015, 5:55 PM), https://www.wired.com/2015/08/happened-hackers-posted-stolen-ashley-madison-data/.

154. Solove & Citron, *supra* note 2, at 764.

155. *See* Jeff Kosseff, *Cybersecurity of the Person*, 17 FIRST AM. L. REV. 343, 366 ("As individuals continue to be victimized online, we need to reimagine cybersecurity laws to address these broader harms. Cybersecurity laws should protect a wider range of data, and they should require manufacturers and service providers to adopt safeguards that protect individuals.").

156. Raphael Satter, *Inside Story: How Russians Hacked the Democrats' Emails*, AP NEWS (Nov. 4, 2017), https://www.apnews.com/dea73efc01594839957c3c9a6c962b8a.

In short, cybersecurity law has been too slow to move beyond the narrow focus on the confidentiality of data that can cause economic harm. While such concerns remain important, the law must catch up with current threats such as revenge pornography, ransomware, deepfakes, foreign attacks on U.S. democracy, and fake news. Accordingly, a successful hacking of U.S. cybersecurity law requires a broad focus on confidentiality, integrity, and availability.

### *E. Cohesive*

Cybersecurity law should be cohesive throughout the United States, recognizing that companies likely will operate nationally. It is difficult—and counterproductive—to subject companies or individuals to a patchwork of inconsistent or conflicting requirements within a single nation.

Unlike some technology-specific fields such as patent law, which is exclusively in the domain of federal laws,[157] cybersecurity law in the United States is governed both at the federal and state levels.[158] As explained in Part II, cybersecurity law encompasses not only national security-related statutes, but tort and criminal law, much of which is inherently a creature of state law.[159] These statutes and common law rules developed decades or centuries before "cybersecurity" was a household term,[160] so it is understandable that the law is dispersed at the state and federal levels.

Cybersecurity does not recognize the traditional boundaries of states or countries. As Electronic Frontier Foundation founder John Perry Barlow wrote in the 1996 Declaration of the Independence of Cyberspace, a call against government interference in the developing Internet:

> Governments derive their just powers from the consent of the governed. You have neither solicited nor received ours. We did not invite you. You do not know us, nor do you know our world. Cyberspace does not lie within your borders. Do not think that you can build it, as though it were a public construction project.[161]

Indeed, the borders that existed for much of commerce before the Internet have largely fallen. A New York-based website likely processes data on residents of all fifty states and conducts some level of business there, and therefore could be subject to the cybersecurity and privacy laws of all of those states.[162]

157. *Outline of the Legal and Regulatory Framework for Intellectual Property in the United States of America*, WIPO LEX, https://wipolex.wipo.int/en/info/outline/US (last visited Mar. 23, 2020).

158. *See Defining Cybersecurity Law*, *supra* note 8, at 1010.

159. *Id.* at 988.

160. *Id.*

161. John Perry Barlow, *A Declaration of the Independence of Cyberspace*, ELECTRONIC FRONTIER FOUND (Feb. 8, 1996), https://www.eff.org/cyberspace-independence.

162. *See, e.g.*, *Defining Cybersecurity Law*, *supra* note 8, at 1014–15 ("Because state breach-notification laws apply based on the residency of individuals, companies with customers in all 50 states must sort through each of these laws at a time when they could otherwise be remediating the breach. This can prove to be complex and time-consuming, particularly for small and midsized companies that have small information security and legal teams.").

Some states impose more onerous cybersecurity requirements than others. For instance, fewer than half of the states even have data security laws, and most of them only require "reasonable" measures.[163] Nevada, for instance, requires encryption for certain transfers of its residents' personal information, and compliance with Payment Card Industry Data Security Standards for the processing of its residents' payment card data.[164] Massachusetts's data security regulations are even more granular, specifying requirements of safeguards such as firewalls and security training.[165] These requirements all are laudable, but there is little reason to impose different rules based on the residence of the data subjects. Instead, a more effective system would articulate a consistent standard that applies throughout the United States. This would not only provide companies with clarity as to how they should safeguard information, but it would allow regulators, lawmakers, industry, and consumer advocates to focus their attention on aligning a single set of standards with current threats.

When the Founders provided Congress with the ability to regulate interstate commerce, they sought to avoid such state-by-state regulation of inherently interstate activities.[166] The current approach to cybersecurity law contradicts the vision of a unified commercial framework that the Founders articulated. Consider a company that has just experienced a data breach. Like most companies of a certain size, it does at least some business in all fifty states and the District of Columbia. In the valuable hours after a data breach, it must review all fifty-one breach notification laws, as they apply based on the state of the data subject's residence. Whether the breach notice law applies will depend in part on how the law defines covered "personal information"; many states only cover name in combination with social security number, driver's license number, or full financial account data,[167] but many states add their own preferred categories to those definitions: for instance, North Dakota also covers birth date and mother's maiden name,[168] and Texas includes information about a resident's health care treatment.[169] While there may be valid justifications for notifying individuals about the breach of all of these types of data, there is little justification for the definition to differ based on the data subject's state of residence. Likewise, if the notification requirement is triggered, the precise form and content of the notification will vary by state.[170] Many—but not all—states allow email notification, but some require notification via snail mail.[171] The content also varies: Michigan, for instance, requires companies to describe the incident that led to the data

163. *Data Security Laws: Private Sector*, NAT'L CONFERENCE OF STATE LEGISLATURES (May 29, 2019), http://www.ncsl.org/research/telecommunications-and-information-technology/data-security-laws.aspx.

164. NEV. REV. STAT. ANN. §§ 603A.210–220 (LexisNexis 2019).

165. 201 MASS. CODE REGS. 17.04 (LexisNexis 2019).

166. *See* THE FEDERALIST No. 22 (Hamilton) ("[W]e may reasonably expect, from the gradual conflicts of State regulations, that the citizens of each would at length come to be considered and treated by the others in no better light than that of foreigners and aliens.").

167. *See* JEFF KOSSEFF, CYBERSECURITY LAW 38 (2017).

168. N.D. CENT. CODE § 51-30-01(4)(a)(5)–(6) (2019).

169. TEX. BUS. & COMM. CODE ANN. § 521.002(a)(2)(B)(i) (West 2019).

170. *See* KOSSEFF, *supra* note 167, at 40.

171. *Id.*

breach,[172] while Massachusetts prohibits notices from including a description of the nature of the breach or the number of Massachusetts residents involved.[173]

As I recently argued in a *Wake Forest Law Review* article, *Hamiltonian Cybersecurity,* the disparate (and, in many cases, nonexistent) state cybersecurity requirements described above are difficult to apply in practice, and they contradict the vision of national commercial regulation that the Founders envisioned.[174] Even if it made sense to protect the data of Nevada residents more than that of Idaho residents, such distinctions would be difficult if not impossible for companies to implement, as they tend to store and process data within the same systems, regardless of the data subject's state of residence.[175] The most practical approach for a company seeking to comply with these requirements would be to adopt the strictest of the state requirements and apply them nationwide. Although that solution would address some of the practical difficulties of the disparate state regulations, it would violate the core tenets of our dual-sovereignty system to allow a single state to set the standards of behavior for companies nationwide.[176] Indeed, companies have a strong argument that state regulation of cybersecurity violates the Dormant Commerce Clause.[177]

Congress can address the pragmatic and constitutional concerns about the current system by passing cybersecurity laws that expressly preempt state laws that cover the same topics. Of course, any such change would need to ensure that it did not cause unnecessary harm to cybersecurity regulation and enforcement. For instance, state attorneys general have been among the leaders in bringing cases against companies for inadequate privacy or data security practices, particularly in light of the FTC's limited jurisdiction and resources.[178] For that reason, a federal cybersecurity law should allow state attorneys general to bring actions under the federal law, much like how state attorneys general are empowered to enforce COPPA against online services that violate privacy protections for minors under thirteen years old.[179] This system is effective. In 2018, the New York Attorney General announced a nearly $5 million COPPA settlement with the

172. MICH. COMP. LAWS ANN. §§ 445.63, 445.72(6)(c) (West 2019).

173. MASS. GEN. LAWS ch. 93H, § 3(b) (2019).

174. Jeff Kosseff, *Hamiltonian Cybersecurity*, 54 WAKE FOREST L. REV. 155, 162–69 (2019).

175. *Id.* at 181–82.

176. *See id.* at 178–79 ("State legislators and regulators have gone far beyond the limited cybersecurity requirements of federal law, and imposed far more demanding standards on U.S. companies. These laws impose specific–and often difficult–requirements, and sometimes are not in harmony with one another. The U.S. cybersecurity legal framework is far from the "common direction" for commercial regulation that Hamilton and Madison envisioned.").

177. *Id.* at 205–06 ("[I]t is increasingly likely that courts will apply Dormant Commerce Clause caselaw and find that at least some of the state laws are impermissibly extraterritorial, excessively burdensome, or inconsistent with one another.").

178. *See* Danielle Keats Citron, *The Privacy Policymaking of State Attorneys General*, 92 NOTRE DAME L. REV. 747, 749 (2016) ("State attorneys general have been on the front lines of privacy enforcement since before the intervention of federal agencies.").

179. 15 U.S.C. § 6504(a)(1) (2018). ("In any case in which the attorney general of a State has reason to believe that an interest of the residents of that State has been or is threatened or adversely affected by the engagement of any person in a practice that violates any regulation of the Commission prescribed under section 6502(b) . . . .").

parent company of AOL, in a case involving advertising network data.[180] This fine was the largest ever issued under COPPA at the time.[181] The dual-enforcement allows state attorneys general to approach regulatory requirements with the appropriate level of vigor, while avoiding the creation of fifty different standards.

A national cybersecurity regulatory regime should ensure that private parties can continue to seek to hold companies accountable for cybersecurity incidents via class action litigation. There are some challenges to this avenue that Congress cannot address, such as the increasing reluctance for many courts to find that plaintiffs have suffered the necessary injury in fact[182] to establish Article III standing unless a data breach caused actual financial injury such as identity theft.[183] Assuming that plaintiffs can overcome the standing barrier, cybersecurity litigation (or the threat thereof) can be an effective way to cause companies to improve their cybersecurity safeguards.[184] Little good arises, however, from subjecting data breach litigation claims to the peculiarities of state tort law, much of which dates back centuries and has little relation to cybersecurity. For instance, some—but not all—states have adopted an economic loss rule that prevents recovery in negligence lawsuits for merely financial harms.[185] The practical impact of these disparities is that in large data breach cases that involve individuals in all fifty states, judges must parse through the caselaw of each state to determine whether the plaintiffs have stated a valid claim.[186] For instance, in a 2014 opinion that granted in part and denied in part Target's motion to dismiss a class action lawsuit arising from its high-profile 2013 breach of payment card data, Minnesota Federal Judge Paul A. Magnuson devoted more than 12,000 words to a state-by-state analysis.[187] Such disparate legal rules not only unnecessarily consume judicial resources, but they make it difficult for companies to understand their legal obligations, and for plaintiffs to understand the chances of success of endeavoring to bring a costly lawsuit after a cybersecurity incident.

To balance the need for consistency in civil remedies with the understandable concern that preemption would undercut the efficacy of class actions, any

180. Sapna Maheshwari, *Oath Agrees to $5 Million Settlement Over Children's Privacy Online*, N.Y. TIMES (Dec. 3, 2018), https://www.nytimes.com/2018/12/03/business/media/oath-children-online-privacy.html.

181. *Id.*

182. Whitmore v. Arkansas, 495 U.S. 149, 155 (1990) ("The complainant must allege an injury to himself that is 'distinct and palpable,' as opposed to merely '[a]bstract,' and the alleged harm must be actual or imminent, not 'conjectural' or 'hypothetical.'") (citations omitted).

183. *See, e.g.*, Reilly v. Ceridian Corp., 664 F.3d 38, 42 (3d Cir. 2011) ("Appellants' contentions rely on speculation that the hacker: (1) read, copied, and understood their personal information; (2) intends to commit future criminal acts by misusing the information; and (3) is able to use such information to the detriment of Appellants by making unauthorized transactions in Appellants' names. Unless and until these conjectures come true, Appellants have not suffered any injury; there has been no misuse of the information, and thus, no harm.").

184. *See* Solove & Citron, *supra* note 2, at 781 ("Such lawsuits allow individuals to have a say about which cases are brought. These lawsuits bring out facts and information about blameworthy security practices by organizations. They provide redress to victims, and they act as a deterrent.").

185. Catherine M. Sharkey, *Can Data Breach Claims Survive the Economic Loss Rule?*, 66 DEPAUL L. REV. 339, 346 (2017) ("[T]he extent to which the stranger economic loss rule serves as a formidable barrier to credit card data security breach cases will depend upon the underlying state law: whether or not the state adopts the majority economic loss rule, and how it defines any exceptions thereto.").

186. *See* KOSSEFF, *supra* note 167, at 67.

187. *In re* Target Corp. Data Sec. Breach Litigation, 66 F. Supp. 3d 1154 (D. Minn. 2014).

preemption of state causes of actions must be accompanied by a sufficiently strong federal civil remedy, including statutory damages.

### *F. Global*

Just as cybersecurity threats do not adhere to boundaries between states, they do not stop at national borders. As seen in recent years, some of the most pervasive threats to U.S. cybersecurity have emerged from Russia, North Korea, China, and Iran.[188] U.S. law enforcement efforts to address these threats have been impressive, with former Special Counsel Robert Mueller securing indictments of Russians for spreading election-related fake propaganda on social media[189] and hacking the Democratic National Committee.[190] And the Justice Department in 2018 indicted two Chinese men for participating in Advanced Persistent Threat 10, a Chinese government-affiliated hacking group that stole hundreds of gigabytes of sensitive data from U.S. companies from 2006 to 2018.[191]

Despite the success of the indictments, there is a significant obstacle to the criminal prosecutions: it is highly unlikely that any of the indicted people from China or Russia will ever set foot in a U.S. court. That is because it is unconceivable that China or Russia would extradite people to face trial in the United States, particularly if the defendants acted on behalf of their governments or were in any way associated with their governments. As the FBI noted in its announcement of the China indictments, "Although the two indicted hackers are believed to be in China, they can be arrested if they travel."[192]

For nearly two decades, cybercrime experts around the world have recognized the global nature of cybercrime through the development and ratification of the Convention on Cybercrime, also known as the Budapest Convention.[193] The Convention harmonizes cybercrime laws such as the Computer Fraud and Abuse Act by requiring their analogues in other countries to contain a baseline

188. *See* DANIEL R. COATS, STATEMENT FOR THE RECORD: WORLDWIDE THREAT ASSESSMENT OF THE U.S. INTELLIGENCE COMMUNITY 5 (2018), https://www.dni.gov/files/documents/Newsroom/Testimonies/2018-ATA---Unclassified-SSCI.pdf ("Russia, China, Iran, and North Korea will pose the greatest cyber threats to the United States during the next year. These states are using cyber operations as a low-cost tool of statecraft, and we assess that they will work to use cyber operations to achieve strategic objectives unless they face clear repercussions for their cyber operations. Nonstate actors will continue to use cyber operations for financial crime and to enable propaganda and messaging.").

189. *See* Matt Apuzzo & Sharon LaFraniere, *13 Russians Indicted as Mueller Reveals Effort to Aid Trump Campaign*, N.Y. TIMES (Feb. 16, 2018, 7:36 AM), https://www.nytimes.com/2018/02/16/us/politics/russians-indicted-mueller-election-interference.html.

190. *See* Aruna Viswanatha et al., *Mueller Probe Indicts 12 Russians in Hacking of Democratic National Committee and Clinton Campaign*, WALL ST. J. (July 14, 2018, 7:36 AM), https://www.wsj.com/articles/mueller-probe-indicts-12-russians-in-hacking-of-democratic-national-committee-1531498286.

191. *See Chinese Hackers Indicted: Members of APT 10 Group Targeted Intellectual Property and Confidential Business Information*, FBI (Dec. 20, 2018), https://www.fbi.gov/news/stories/chinese-hackers-indicted-122018.

192. *Id.*

193. COUNCIL OF EUROPE, CONVENTION ON CYBERCRIME (2001), https://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680081561.

of similar offenses.[194] The Convention also provides safeguards for the collection and preservation of evidence of computer crimes.[195] Perhaps most important for cross-border enforcement are its requirements for international cooperation, including extradition of individuals charged with computer crimes.[196] The Budapest Convention has a number of critics, in part because of the lack of teeth in the cooperation provisions and the lack of specificity in some provisions.[197] And even to the extent that the Budapest Convention's substantive and procedural requirements are effective, they are utterly useless for the United States in most cases of cybercrime. That is because China, Iran, North Korea, and Russia are not among the roughly sixty nations to have ratified the Budapest Convention.[198] In other words, the United States has no way of extraditing cybercriminals from the nations that are the most rampant sources of cybercrime against the United States.[199]

It is unlikely that Russia, China, Iran, or North Korea will agree to ratify the Budapest Convention or any other agreement that would subject cyber criminals within their jurisdiction to international prosecution. This means that the United States cannot merely rely on the existing network of cybercrime statutes, such as the CFAA,[200] to blunt the increasing force of global cyberattacks. The United States can—and should—use diplomacy and international alliances to pressure cyber adversaries to cease or reduce this malicious behavior.[201] Moreover, the United States should continue to take aggressive actions to deter attacks from other countries, both by building its defenses and imposing costs on attackers. For instance, the U.S. military's cyber policy is increasingly aggressive, with a strategy of "persistent engagement," which "focuses on an aggressor's confidence and capabilities by defending against, countering, and contesting on-going strategic campaigns short of armed attack."[202] To implement its persistent engagement strategy, the United States has developed a new operational concept,

194. *Id.*

195. *Id.*

196. *Id.*

197. *See* JACK GOLDSMITH, CYBERSECURITY TREATIES: A SKEPTICAL VIEW 3 (2011) ("The Cybercrime Convention is widely viewed as unsuccessful. It achieved 'consensus' on computer crimes only by adopting vague definitions that are subject to different interpretations by different states. Even with vague definitions, many nations conditioned their consent on declarations and reservations (the United States had more than a half dozen) that further diluted the scope of covered crimes, making the treaty's obligations even less uniform and less demanding.").

198. *See Chart of Signatures and Ratifications of Treaty 185: Convention on Cybercrime*, COUNCIL OF EUROPE, https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures (last visited Mar. 23, 2020).

199. *See* Jeff Kosseff, Developing Collaborative and Cohesive Cybersecurity Legal Principles, Proceedings of the 2018 International Conference on Cyber Conflict (2018) ("The Budapest Convention is of limited utility because many of the most pernicious attacks are perpetrated from nations that are not parties to the Convention; laws that effectively promote the cybersecurity of public and private systems and networks, however, provide incremental worldwide benefits, even if they have not been adopted by the handful of nations that are the sources of the attacks.").

200. *Id.*

201. *See generally* André Barrinha & Thomas Renard, *Cyber-Diplomacy: The Making of an International Society in the Digital Age*, 3 J. GLOBAL AFF. 353 (2017).

202. U.S. CYBER COMMAND, CYB3R CYPH3RS: DATA. INFORMATION. KNOWLEDGE 5 (2018).

"Defend Forward."[203] U.S. Cyber Command, in a March 2018 high-level vision document, described the concept as "[d]efending forward as close as possible to the origin of adversary activity extends our reach to expose adversaries' weaknesses, learn their intentions and capabilities, and counter attacks close to their origins."[204] These actions are part of a two-pronged strategy to deter adversarial cyber behavior by denial (making the attacks more difficult to succeed) and cost imposition (inflicting negative consequences on the attacker).[205] This more aggressive posture is generally within the confines of international law of war, as it does not rise to the level of use of force or armed attack,[206] and it could be an effective way to reduce the success of global cyberthreats that are unconstrained by traditional computer hacking laws.[207]

Additionally, the United States can defend against global cyberthreats by bolstering the defenses of both the public and private sectors. The United States has increasingly focused on improving public sector defenses, particularly in light of the 2015 revelation of China's theft of millions of U.S. security clearance applications from the Office of Personnel Management.[208] The Defense Department and National Archives, for instance, rolled out new regulations to better secure "controlled unclassified information," which is unclassified information that nonetheless "requires safeguarding or dissemination controls pursuant to and consistent with applicable law, regulations, and government-wide policies."[209] The federal government has exercised less direct control over the security of *private sector* information and systems, but as explained above, that could change with comprehensive federal data security legislation and accompanying regulations.[210] Such new requirements should incorporate the government's understanding of the most persistent and dangerous global cybersecurity threats.

U.S. cybersecurity law also must recognize the requirements that other nations and jurisdictions impose on securing data. For instance, in 2018, the European Union's General Data Protection Directive ("GDPR") went into effect.[211]

203. *Id.*

204. U.S. CYBER COMMAND, ACHIEVE AND MAINTAIN CYBERSPACE SUPERIORITY: COMMAND VISION FOR US CYBER COMMAND 6 (2018).

205. *See generally* Aaron F. Brantly, *The Cyber Deterrence Problem*, presented to the 2018 International Conference on Cyber Conflict (2018).

206. *See* TALLINN MANUAL 2.0 ON THE INTERNATIONAL LAW APPLICABLE TO CYBER OPERATIONS 333 (Michael N. Schmitt ed., 2d ed. 2017).

207. *See* Jeff Kosseff, The Contours of 'Defend Forward' Under International Law, proceedings of the 2019 International Conference on Cyber Conflict (2019) ("Defend Forward is the clearest indication of the U.S. recognition that cyber threats do not merely take the form of discrete events but are also continuous operations that must be defended against in real time.").

208. *See* Shane Harris, *Team Obama Knows China Is Behind the OPM Hack. Why Won't They Say So?*, DAILY BEAST (Apr. 14, 2017, 10:17 AM), https://www.thedailybeast.com/team-obama-knows-china-is-behind-the-opm-hack-why-wont-they-say-so.

209. *About Controlled Unclassified Information (CUI)*, NAT'L ARCHIVES, https://www.archives.gov/cui/about (last visited Mar. 23, 2020).

210. *See supra* Part II.

211. Regulation 2016/679 of the European Parliament and of the Council of Apr. 27, 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation), art. 99, 2016 O.J. L 119/1 [hereinafter *GDPR*].

While the law is a data protection law that provides a number of obligations not tied solely to cybersecurity—such as data subject access and the right of a data subject to have data erased—the directive also requires companies to implement "appropriate technical and organisational measures to ensure a level of security appropriate to the risk."[212] GDPR provides examples such as pseudonymization, encryption, and regular security testing,[213] and some regulators have provided more detailed guidance of complying with GDPR's security requirements.[214] GDPR applies not only to companies established in the European Union, but also to those that offer goods or services "irrespective of whether a payment of the data subject is required, to such data subjects in the Union," or those that monitor "behaviour as far as their behaviour takes place within the Union."[215] Accordingly, many U.S. companies, even those without any physical presence in Europe, must comply with GDPR because they target or monitor certain individuals who are located in Europe. Of course, these companies are only required to comply with GDPR for the data regarding individuals who are located in Europe,[216] but it may be impractical to segregate data storage systems. Thus, GDPR may influence the security safeguards that U.S. companies apply to individuals in the United States. If Congress enacts a comprehensive privacy, data protection, and data security statute, it should consider such global standards to ensure that they are properly aligned with the new U.S. requirements.

### *G. Collaborative*

The United States has centralized agencies or departments for many legal areas: taxes (Internal Revenue Service), securities regulation (Securities and Exchange Commission), and transit safety (Transportation Department), to name a few.

What about cybersecurity? Those responsibilities are more scattered across departments and independent agencies. At the federal level alone: the Department of Homeland Security is home to the recently renamed and revamped Cybersecurity and Infrastructure Security Agency ("CISA"),[217] which is responsible for federal civilian government cybersecurity. The DHS agency also houses the National Cybersecurity and Communications Integration Center, which operates a round-the-clock incident response center and shares threat information with the private sector.[218] A great deal of the U.S. government's cybersecurity

212. *Id.* art. 32(1), at 51.

213. *Id.* art. 32(1), at 51–52.

214. *See. e.g.*, *Guide to the General Data Protection Regulation (GDPR)*, INFO. COMMISSIONER'S OFF., https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/security/ (last visited Mar. 23, 2020) ("The security principle goes beyond the way you store or transmit information. Every aspect of your processing of personal data is covered, not just cybersecurity.").

215. *GDPR*, *supra* note 211, art. 3(2), at 33.

216. *Id.*

217. Cybersecurity and Infrastructure Security Agency Act, H.R. 3359, 115th Cong. § 2 (2018).

218. *See National Cybersecurity and Communications Integration Center*, DEP'T OF HOMELAND SECURITY, https://www.dhs.gov/national-cybersecurity-and-communications-integration-center (last visited Mar. 23, 2020) ("The National Cybersecurity and Communications Integration Center's (NCCIC) mission is to reduce the risk

expertise, however, is not in CISA's Arlington, Virginia headquarters, but miles away in Ft. Meade, Maryland, at the headquarters of the National Security Agency and U.S. Cyber Command. NSA, which is the government's signals intelligence agency, and U.S. Cyber Command, which is the military's cyber combatant command, are housed in the same location and report to the same director/commander, though their employees have very different functions.[219] Both, however, are home to some of the government's most skilled cybersecurity professionals, and gather information about global cyber threats that threaten the United States.[220]

Cybersecurity, however, goes far beyond Arlington and Ft. Meade. The National Institute of Standards and Technology ("NIST"), part of the U.S. Commerce Department, sets a wide range of standards for cybersecurity that are used throughout the public and private sectors.[221] NIST also has developed a Cybersecurity Framework,[222] which articulates a five-step process for public and private-sector organizations to develop cybersecurity plans (Identify, Protect, Detect, Respond, and Recover).[223] The Framework has been hailed by experts throughout government and industry as an innovative and useful contribution to the understanding of how to bolster cybersecurity defenses and prepare for inevitable incidents.[224] Other cybersecurity resources are located in the Justice Department.[225] The FBI has a skilled cybersecurity division that is charged with

of systemic cybersecurity and communications challenges in our role as the Nation's flagship cyber defense, incident response, and operational integration center.").

219. *See* Mark Pomerleau, *DoD Quietly Reorganizes Cyber Command*, FIFTH DOMAIN (Jan. 9, 2018), https://www.fifthdomain.com/dod/cybercom/2018/01/09/dod-quietly-reorganizes-cyber-command-to-shepherd-command-through-elevation/; *Paul M. Nakasone*, NAT'L SECURITY AGENCY, https://www.nsa.gov/About-Us/Current-Leadership/Article-View/Article/1596277/paul-m-nakasone/About-Us/EEO-Diversity/Employee-Resource-Groups/ (last visited Mar. 23, 2020).

220. *See* Darren Samuelsohn, *Inside the NSA's Hunt for Hackers*, POLITICO (Dec. 9, 2015, 4:56 AM), https://www.politico.com/agenda/story/2015/12/federal-government-cyber-security-technology-worker-recruiting-000330 ("The NSA is among the most aggressive agencies in government for pursuing new cyber talent, and clearly it has some pull: potential applicants stood two and sometimes three deep in Baltimore, curious about what life just might be like working for an agency central to the country's intelligence gathering operations, and which also is still struggling to rebuild its reputation after being front and center in the Edward Snowden scandal.").

221. *See Cybersecurity*, NAT'L INST. OF STANDARDS & TECH., https://www.nist.gov/topics/cybersecurity (last visited Mar. 23, 2020).

222. *See Cybersecurity Framework*, NAT'L INST. OF STANDARDS & TECH., https://www.nist.gov/cyberframework (last visited Mar. 23, 2020).

223. *Id.*

224. *See, e.g.*, George Wrenn, *Adopt the NIST Cybersecurity Framework [CSF] and harness the Wisdom of Crowds*, CSO (May 2, 2018, 5:50 AM), https://www.csoonline.com/article/3269532/adopt-the-nist-cybersecurity-framework-csf-and-harness-the-wisdom-of-crowds.html ("I would argue that the NIST CSF is the most robust yet understood framework to date. It covers five critical framework functions: Identify, Protect, Detect, Respond and Recover – all critical parts that require controls, policies, and procedures within your organization both inside and outside of your cybersecurity team."); *The Benefits of the Latest Cybersecurity Framework*, CIO APPLICATIONS (Nov. 30, 2018), https://www.cioapplications.com/news/the-benefits-of-the-latest-cybersecurity-framework-nid-2149.html ("This NIST Cybersecurity Framework is the most comprehensive best practices to be applied when planning to implement a cybersecurity framework or standard.").

225. *Cybersecurity Unit*, U.S. DEP'T OF JUST., https://www.justice.gov/criminal-ccips/cybersecurity-unit (last updated Mar. 12, 2020).

being the lead federal agency to direct "threat response" activities after a significant cybersecurity incident.[226]

While DHS, NSA, Cyber Command, FBI, and NIST have significant cybersecurity expertise and some notable successes, they are not involved with regulating the cybersecurity of private companies.[227] In fact, it is not always completely clear which federal agencies have the authority to enforce cybersecurity standards for companies. The FTC is the closest thing to a general cybersecurity regulator that the United States has, but as described above, its enforcement authority is limited primarily to bringing enforcement actions and reaching consent decrees with companies, requiring them to adopt stronger security safeguards.[228] Although the FTC has suggested in a blog post that companies take safeguards such as the NIST Cybersecurity Framework,[229] it has not formally adopted as regulations or safe harbors the NIST Framework (or any other safeguards, for that matter).

The FTC is not the only federal agency that regulates cybersecurity. The Gramm Leach Bliley Act,[230] which requires safeguards for financial institutions' nonpublic information, is enforced not only by the FTC, but by each of the financial regulators: the Office of Comptroller of the Currency, Federal Reserve Board, Federal Deposit Insurance Corporation, Office of Thrift Supervision, Securities and Exchange Commission, Commodity Futures Trading Commission, National Credit Union Administration, and Federal Trade Commission.[231] While some of the agencies have adopted a common set of guidelines to implement GLBA,[232] others, such as the NCUA,[233] FTC,[234] and SEC,[235] have adopted their

226. *See* The White House, Presidential Policy Directive 41--United States Cyber Incident Coordination (July 26, 2016), https://obamawhitehouse.archives.gov/the-press-office/2016/07/26/presidential-policy-directive-united-states-cyber-incident ("Threat response activities include conducting appropriate law enforcement and national security investigative activity at the affected entity's site; collecting evidence and gathering intelligence; providing attribution; linking related incidents; identifying additional affected entities; identifying threat pursuit and disruption opportunities; developing and executing courses of action to mitigate the immediate threat; and facilitating information sharing and operational coordination with asset response.").

227. *See supra* Section III.A.

228. *See* Nuala O'Connor, *Reforming the U.S. Approach to Data Protection and Privacy,* COUNCIL ON FOREIGN REL. (Jan. 30, 2018), https://www.cfr.org/report/reforming-us-approach-data-protection ("The FTC has the general power to prohibit 'unfair and deceptive trade practices' under Section 5 of the FTC Act, and has attempted to establish a data-security baseline through over sixty different enforcement actions. However, companies have begun to aggressively push back against the FTC's legal authority to police data-security practices, and the FTC has limited jurisdiction over banks, insurance companies, nonprofit entities, and even some internet service providers.").

229. Andrea Arias, *The NIST Cybersecurity Framework and the FTC*, FED. TRADE COMM'N (Aug. 31, 2016, 2:34 PM), https://www.ftc.gov/news-events/blogs/business-blog/2016/08/nist-cybersecurity-framework-ftc ("The Framework's five Core functions can serve as a model for companies of all sizes to conduct risk assessments and mitigation, and can be used by companies to: (1) establish or improve a data security program; (2) review current data security practices; or (3) communicate data security requirements with stakeholders.").

230. The Gramm Leach Bliley Act, 15 U.S.C. § 6801 (2018).

231. *Id.* §§ 6801, 6805.

232. *See* Interagency Guidelines Establishing Standards for Safety and Soundness, appendix D-1 to 12 C.F.R. § 208.

233. 12 C.F.R. § 248 (2019).

234. 16 C.F.R. § 314 (2019).

235. 17 C.F.R. § 248.30 (2019).

own GLBA regulations. The Department of Health and Human Services regulates the security of healthcare information under the Health Insurance Portability and Accountability Act,[236] the Federal Energy Regulatory Commission regulates the cybersecurity of the bulk power system,[237] and the Nuclear Regulatory Commission regulates the cybersecurity of nuclear power facilities,[238] to name a few industry-specific regulations (and that is not even including the many state-focused cybersecurity regulations, such as New York's rules for financial institutions[239] and South Carolina's new requirements for insurers).[240]

In short, many agencies with different leaders and different agendas are charged with shaping U.S. cybersecurity policy, strategy, and enforcement. Some of this dispersion is to be expected; for instance, the Posse Comitatus Act[241] prevents the military from enforcing civilian criminal laws and conducting civilian criminal investigations, though it allows some non-enforcement assistance to civilian governments.[242] When possible, however, cybersecurity functions should be housed within the same department or agency to allow a better alignment among both regulations and assistance. For instance, if NIST is housed within the same department that regulates private-sector cybersecurity, the regulatory unit might be more inclined to formally adopt the NIST Cybersecurity Framework as a standard of care. Moreover, a cybersecurity-focused agency would be more likely to have a wider range of expertise and updated knowledge about the current and future cybersecurity threats. Just as the United States created the Department of Homeland Security to centralize functions after the September 11 terrorist attacks, it is facing increasing calls to create something akin to a federal "Department of Cybersecurity" in light of the persistent cybersecurity challenges,[243] though such proposals have received reasoned criticism for threatening to slow the progress that the United States has made on cybersecurity, and potentially discouraging other agencies from focusing on cybersecurity.[244]

236. 45 C.F.R. § 160.103 (2018).

237. 18 C.F.R. § 40 (2007).

238. 10 C.F.R. § 73.54 (2015).

239. N.Y. COMP. CODES R. & REGS. tit. 23 § 500 (2011).

240. South Carolina Insurance Data Security Act, H.R. 4655, 122nd Sess. (S.C. 2018).

241. 18 U.S.C. § 1385 (2018).

242. *See* United States v. Dreyer, 804 F.3d 1266, 1275 (9th Cir. 2015) (en banc) ("PCA-like restrictions prohibit direct military involvement in civilian law enforcement activities, but they permit some indirect assistance, such as involvement that arises during the normal course of military operations or other actions that do not subject civilians to the use of military power that is regulatory, prescriptive, or compulsory.").

243. *See, e.g.*, Ted Schlein, *The United States Needs a Department of Cybersecurity*, TECHCRUNCH (Apr. 16, 2018, 8:35 AM), https://techcrunch.com/2018/04/16/the-united-states-needs-a-department-of-cybersecurity/ ("What is needed is a sixteenth branch of the Executive—a Department of Cybersecurity—that would assemble the country's best talent and resources to operate under a single umbrella and a single coherent policy. By uniting our cyber efforts we would make the best use of limited resources and ensure seamless communications across all elements dealing in cyberspace. The department would act on behalf of the government and the private sector to protect against cyberthreats and, when needed, go on offense.").

244. *See* Suzanne Spaulding & Mieke Eoyang, *Bad Idea: Creating a U.S. Department of Cybersecurity*, DEFENSE360 (Dec. 13, 2018), https://defense360.csis.org/bad-idea-creating-a-u-s-department-of-cybersecurity/ ("We cannot stovepipe thinking about cybersecurity into one centralized place or approach. The threat is so pervasive and so severe that it requires a recognition that a change in thinking is necessary for everyone operating

Even if these logistical and pragmatic concerns prevent centralization of cybersecurity into a single federal department, policymakers should at the very least attempt to better coordinate cybersecurity efforts across the government. One model for consideration would be a cybersecurity equivalent of the Director of National Intelligence, which was created in 2004.[245] Although the sixteen intelligence agencies are not within the Office of the Director of National Intelligence (the NSA, for instance, remains in the Department of Defense, and the Bureau of Intelligence and Research remains in the State Department), the Director's mission is to lead the intelligence community by "effectively operating as one team: synchronizing collection, analysis and counterintelligence so that they are fused."[246] A similar cybersecurity-focused office, with sufficient authority and resources, could provide the necessary coordination and expertise-sharing necessary to better combat cybersecurity threats.

Centralization of cybersecurity functions would also allow a more effective and continuous evaluation of government efforts to battle cybersecurity threats and mitigate harms. Currently, there is little whole-of-government coordination of these efforts, as the functions are scattered across so many federal and state agencies and departments.[247] Although measuring the success of government programs is not an easy task—particularly when the challenges and threats are as persistent as they are in cyberspace—a centralized coordination effort could at least attempt to develop metrics to evaluate the success (or lack thereof) of government efforts, as well as trends in the threats that the United States faces.

Moreover, we must look beyond only government if we want to truly improve the cybersecurity rules and standards by which companies operate. Cybersecurity law would benefit from a more robust application of the polycentric governance model to cybersecurity. Polycentric governance is "a system of governance in which authorities from overlapping jurisdictions (or centers of authority) interact to determine the conditions under which these authorities, as well as the citizens subject to these jurisdictional units, are authorized to act as well as the constraints put upon their activities for public purposes."[248] As Scott Shackelford et al. explored in an excellent recent piece about Internet of Things security, polycentric governance "could help move the debate regarding the Security of Things in a more productive direction as part of an overarching campaign to promote some measure of cyber peace."[249] They persuasively make the case for a *coordinated* system of self-regulation by companies, incentives, and

an enterprise–from the app developer in their dorm room, to the mission or business operator, to the President of the United States.").

245. *Id.*; 50 U.S.C. § 3023 (2018).

246. *Mission, Vision & Values*, OFF. OF THE DIRECTOR OF NAT'L INTELLIGENCE, https://www.dni.gov/index.php/who-we-are/mission-vision (last visited Mar. 23, 2020).

247. *See supra* notes 230–44 and accompanying text.

248. Scott Shackelford et al., *When Toasters Attack: A Polycentric Approach to Enhancing the "Security of Things"*, 2017 U. ILL. L. REV. 415, 419 n.20 (2017) (quoting Michael D. McGinnis, *An Introduction to IAD and the Language of the Ostrom Workshop: A Simply Guide to a Complex Framework*, 39 POL'Y STUD. J. 169, 171 (2011)).

249. *Id.* at 420.

government regulation.[250] As policymakers and industry continue to hack the broader system of cybersecurity law, they should keep in mind the need for a cohesive polycentric system of governance that recognizes the urgency of aligning shared goals and values to strengthen cybersecurity.

## IV. CONCLUSION

In *Defining Cybersecurity Law*, I provided a proposal for a common definition for cybersecurity law and highlighted what I viewed as the most urgent shortcomings in that legal framework. In short, the cybersecurity system needs to be hacked. It requires radical change to better align the many different areas of the law with a common goal: protecting the confidentiality, integrity, and availability of information, systems, and networks in the public and private sector. The hack must position U.S. laws to address not only the imminent cybersecurity threats that we currently face, but it also must provide sufficient flexibility to effectively fight future threats.

Easier said than done. Because U.S. cybersecurity law spans so many different areas of federal and state law, executing this hack is not an easy task. It would be foolhardy and presumptuous to list a narrow set of discrete proposals to "fix" the broken cybersecurity legal system. Such work may come down the line, but the first task is to better understand what we want our cybersecurity laws to look like. The hack requires a set of common values and principles to guide policymaking at the state, federal, and global level. This Article has suggested a set of such values and principles to guide policymakers as they attempt to better safeguard the public and private sectors from constantly evolving cybersecurity threats.

With this Article, I hope to expand on high-level, normative goals that policymakers may apply in their efforts to better align our laws, policies, and government programs with the threats to national security, the economy, and individuals. Future research will develop specific solutions (either through legislation, regulation, or procedure), that will implement the goals articulated in this Article.

250. *Id.* at 469–71 ("Consequently, while it is true that the desire for industry self-regulation seems justified, given the still nascent state and rapid development of the underlying technologies, some IoT regulation may in fact be necessary, especially in critical areas of concern, such as transportation and healthcare. Regulation, however, should be limited to at-risk areas or populations (such as children), and it should be crafted to reinforce existing best-practice frameworks, as has arguably happened in the electricity regulatory context. Most important to a self-regulatory model, policy-makers must create incentives to encourage the further refinement of best practices as part of an ecosystem of information-system participants.").