Defining Cybersecurity Law

Jeff Kosseff *

ABSTRACT: As data breaches, denial-of-service attacks, and other cybersecurity incidents lead to extraordinary economic and national security consequences, commentators increasingly look to the legal system for solutions. Unfortunately, U.S. laws do not have a unified and coherent vision for the regulation and promotion of cybersecurity. For that matter, the U.S. legal system lacks a consistent definition of the term "cybersecurity law."

This Article aims to fill that gap by defining "cybersecurity law." Although many articles have addressed various aspects of cybersecurity, none has stepped back to define exactly what "cybersecurity" is and the goals of statutes and regulations that aim to promote cybersecurity. By defining the scope and goals of this new legal field, policymakers can then examine how lawmakers could improve existing laws. Part II of this Article briefly describes the cybersecurity challenges that the United States faces by examining the cyberattack on Sony Pictures Entertainment. Part III defines "cybersecurity law" as a legal framework that "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." Part IV explains the current legal regime for cybersecurity and concludes that many of the most prominent cybersecurity laws only address a small portion of the broader legal framework. Part V examines the gaps in current U.S. cybersecurity law and suggests starting points for improvements.

* Assistant Professor of Cybersecurity Law, United States Naval Academy. J.D., Georgetown University Law Center; M.P.P., B.A., University of Michigan. The views expressed in this Article are only those of the Author and do not represent the views of the United States Naval Academy, Department of Navy, or Department of Defense. Thanks to LCDR Joseph Hatfield, Chris Inglis, Martin Libicki, and other colleagues at the Naval Academy's Cyber Science Department for frequent discussions on the issues covered in the article, and to the staff of the *Iowa Law Review* for their excellent editorial work.

I. INTRODUCTION

In late 2015, after years of attempts, Congress passed legislation to enable companies to voluntarily share information about cybersecurity threats—such as attempted hacks—with the federal government and other companies. The bill, entitled the Cybersecurity Act of 2015, was tucked into a massive omnibus appropriations bill as Division N.[1] The Cybersecurity Act occupies 136 of the 2,009 pages in the omnibus bill, and it in detail establishes rules for operators of private networks to defend their networks, monitor possible threats, and collaborate with the federal government.[2] The new law also bolsters the Department of Homeland Security's ("DHS") cybersecurity efforts. The focus of the legislation, not surprisingly, is cybersecurity; indeed, "cybersecurity" appears in the bill nearly 200 times.[3]

There is just one problem: The Cybersecurity Act does not define "cybersecurity." The statute allows companies to take certain actions for a

1. Cybersecurity Act of 2015, Pub. L. No. 114-113, Div. N, § 1(a), 129 Stat. 2935 (codified at 6 U.S.C.A. §§ 1501–10 (West 2016)).

2. *Id.*

3. *Id.*

"cybersecurity purpose," which it defines as "the purpose of protecting an information system or information that is stored on, processed by, or transiting an information system from a cybersecurity threat or security vulnerability."[4] The statute defines "security vulnerability" as "any attribute of hardware, software, process, or procedure that could enable or facilitate the defeat of a security control."[5] The statute defines "cybersecurity threat" as

> an action, not protected by the First Amendment to the Constitution of the United States, on or through an information system that may result in an unauthorized effort to adversely impact the security, availability, confidentiality, or integrity of an information system or information that is stored on, processed by, or transiting an information system.[6]

The statute also defines "security control,"[7] "malicious cyber command and control,"[8] and "cyber threat indicator."[9] Although these definitions help to illuminate the purpose of the legislation, the Cybersecurity Act does not directly explain what lawmakers meant by "cybersecurity."

The statute fails to provide a concrete definition that sets forth the scope and goals of cybersecurity law. Although the new statute can function without the definition—and as described in Part III of this Article, is a significant improvement over existing law—its omission of this key definition is illustrative of a larger problem: When policymakers talk about cybersecurity, they are not always talking about the same concept.

A day rarely passes without another report of a major cybersecurity incident. Hackers routinely breach the systems of retailers, stealing consumer credit card data, social security numbers, and other valuable personal information.[10] Attackers launch distributed denial-of-service attacks, knocking some of the most popular websites offline for hours or days.[11] Home security

4. 6 U.S.C.A. § 1501(4).

5. *Id.* § 1501(17).

6. *Id.* § 1501(5)(A).

7. *Id.* § 1501(16) ("The term 'security control' means the management, operational, and technical controls used to protect against an unauthorized effort to adversely affect the confidentiality, integrity, and availability of an information system or its information.").

8. *Id.* § 1501(11) ("The term 'malicious cyber command and control' means a method for unauthorized remote identification of, access to, or use of, an information system or information that is stored on, processed by, or transiting an information system.").

9. *Id.* § 1501(6) (listing eight types of threat indicators).

10. *See, e.g.*, David Meyer, *Eddie Bauer is Latest Retailer Infected with Data Breach Malware*, FORTUNE (Aug. 19, 2016), http://fortune.com/2016/08/19/eddie-bauer-data-breach (describing how a malware attack compromised credit card information of Eddie Bauer customers).

11. *See, e.g.*, Lily Hay Newman, *What We Know About Friday's Massive East Coast Internet Outage*, WIRED (Oct. 21, 2016, 1:04 PM), https://www.wired.com/2016/10/internet-outage-ddos-dns-dyn (describing attack on Dyn, a Domain Name Service, which caused websites around the world to be unavailable for much of a day).

webcams become remote spying devices.[12] Even the U.S. electoral system is compromised by hacks of the email accounts of political officials and attacks on state elections systems.[13] In the increasingly frequent news coverage of these attacks, commentators, and lawmakers demand immediate and swift legal solutions to prevent further damage.[14] The constant media coverage begs the question: How well do our existing laws address cybersecurity threats?

The short answer: Not well at all. The slightly longer answer: The patchwork of U.S. statutes and regulations that constitute cybersecurity law is an uncoordinated mishmash of requirements that mostly were conceived long before modern cyber-threats. Modern U.S. cybersecurity law stems from century-old privacy norms, torts, and criminal laws that bear little relation to the protection of the confidentiality, integrity, or availability of systems, networks, and data.

In short, the U.S. legal system lacks a consistent definition of the term "cybersecurity law." This Article aims to fill that gap by defining "cybersecurity law." Although "cybersecurity" is a commonly used term in legal circles, no scholarship has stepped back to define exactly what "cybersecurity law" is and the goals of statutes and regulations that aim to promote "cybersecurity." By defining the scope and goals of this new legal field, policymakers can then examine how lawmakers could improve existing laws. Part II of this Article briefly describes the cybersecurity challenges that the United States faces by examining the cyberattack on Sony Pictures Entertainment. Part III broadly examines current cybersecurity threats to the United States and defines "cybersecurity law" as a legal framework that "promotes the confidentiality, integrity, and availability of public and private information, systems, and networks, through the use of forward-looking regulations and incentives, with

12. *See* Taylor Martin, *How to Prevent Your Security Camera from Being Hacked*, CNET (Aug. 22, 2016, 9:10 AM), https://www.cnet.com/how-to/how-to-prevent-your-security-camera-from-being-hacked ("'Internet of things' devices pose a threat that their non-connected counterparts never did. They increase the number of gateways into your home by introducing vulnerabilities that didn't exist previously.").

13. *See, e.g.*, Joe Uchill, *Typo Led to Podesta Email Hack: Report*, HILL (Dec. 13, 2016, 4:00 PM), http://thehill.com/policy/cybersecurity/310234-typo-may-have-caused-podesta-email-hack (discussing the hack of Hillary Clinton's 2016 presidential campaign chairman John Podesta's email account).

14. *See* Rudy Takala, *Rep. Lieu Demands Answers on Weak Federal Cybersecurity*, WASH. EXAMINER (Sept. 28, 2016, 12:45 PM), http://www.washingtonexaminer.com/rep-lieu-demands-answers-on-weak-federal-cybersecurity/article/2603089 ("A congressional leader on cybersecurity is seeking to find out why federal agencies have failed to implement measures that would improve their cybersecurity posture against the growing volume of cyberattacks against government."); Craig Timberg, *Lawmakers Demand Accounting from Equifax on Massive Security Breach*, WASH. POST (Sept. 11, 2017), https://www.washingtonpost.com/business/technology/lawmakers-demand-accounting-from-equifax-on-massive-security-breach/2017/09/11/733ddf58-9728-11e7-82e4-f1076f6d6152_story.html ("A sternly worded letter from the top Republican and Democrat on the Senate Finance Committee included a list of 13 questions intended to illuminate the murky circumstances surrounding the breach, including what data was exposed, how the hack was detected and whether the company has systems adequate for detecting and thwarting such intrusions.").

the goal of protecting individual rights and privacy, economic interests, and national security." Part IV of this Article explains the current U.S. legal regime for cybersecurity and concludes that many of the most prominent cybersecurity laws only address a small portion of the broader legal framework. Part V examines the gaps in current U.S. cybersecurity law and suggests which areas of cybersecurity law policymakers could better address.

One might argue that it is unnecessary to define a legal field. By proposing a definition of "cybersecurity law," I seek to offer the definition as a broad taxonomy for policymakers and courts as they develop statutes, regulations, and court rulings that could shape cybersecurity for generations to come. By defining "cybersecurity law," I suggest the types of subjects that the law seeks to secure, the methods by which cybersecurity law protects those subjects, and the reasons behind cybersecurity law. Moreover, I intend this definition to do more than merely add to a legal taxonomy; a clear definition of "cybersecurity law" will provide policymakers with goals and guideposts as they debate new laws to protect information, systems, and networks.

II. THE SONY HACK: A CASE STUDY IN U.S. CYBERSECURITY CHALLENGES

Defining "cybersecurity law" requires an examination of the harms that the law seeks to prevent. Understanding those harms is essential to prioritizing the goals, limits, and scope of cybersecurity law. To gain a fuller picture of these issues, it is helpful to review the various harms caused by a modern-day cybersecurity attack. This picture is best illustrated by an examination of one of the highest-profile cyberattacks—the Sony Pictures hack.

In 2014, Sony executives received phishing emails, which contained the link to a falsified site that purported to belong to Apple.[15] The email instructed them to enter their Apple login credentials into a verification form.[16] After some of the Sony executives entered these credentials, hackers used the information to determine the executives' login credentials for Sony's internal networks.[17] The hackers used these credentials to steal large amounts of internal emails and other confidential data, as well as install malware on

15. David Bisson, *Sony Hackers Used Phishing Emails to Breach Company Networks*, TRIPWIRE (Apr. 22, 2015), https://www.tripwire.com/state-of-security/latest-security-news/sony-hackers-used-phishing-emails-to-breach-company-networks. "Phishing is an attempt by an individual or group to solicit personal information from unsuspecting users by employing social engineering techniques. Phishing emails are crafted to appear as if they have been sent from a legitimate organization or known individual." *Report Phishing Sites*, U.S. COMPUTER EMERGENCY READINESS TEAM, https://www.us-cert.gov/report-phishing (last visited Dec. 20, 2017).

16. Bisson, *supra* note 15.

17. *Id.*

Sony's systems that deleted data and paralyzed its operations.[18] As Fortune magazine described in a detailed account of the hack:

> [S]tarting at about 7 a.m. Pacific time on Monday, Nov. 24—a crushing cyberattack was launched on Sony Pictures. Employees logging on to its network were met with the sound of gunfire, scrolling threats, and the menacing image of a fiery skeleton looming over the tiny zombified heads of the studio's top two executives.
>
> Before Sony's IT staff could pull the plug, the hackers' malware had leaped from machine to machine throughout the lot and across continents, wiping out half of Sony's global network. It erased everything stored on 3,262 of the company's 6,797 personal computers and 837 of its 1,555 servers. To make sure nothing could be recovered, the attackers had even added a little extra poison: a special deleting algorithm that overwrote the data seven different ways. When that was done, the code zapped each computer's startup software, rendering the machines brain-dead.
>
> From the moment the malware was launched—months after the hackers first broke in—it took just one hour to throw Sony Pictures back into the era of the Betamax. The studio was reduced to using fax machines, communicating through posted messages, and paying its 7,000 employees with paper checks.[19]

The breach threatened not only Sony's internal productivity and compromised employee privacy; it was also a public relations nightmare. The hackers released highly confidential internal information, including salary data and highly embarrassing emails about movie stars.[20] Sony was criticized for having only 11 information-security employees.[21] Media reports quickly noted a Sony executive's 2007 public comment that he would not invest "$10 million to avoid a possible $1 million loss."[22] A 2015 SANS Institute paper concluded that Sony could have prevented the hack by adopting a few common security safeguards.[23]

18. David Bisson, *Wiper Malware Behind Sony Hack Illustrates the Importance of Risk Management*, TRIPWIRE (Dec. 4, 2014), https://www.tripwire.com/state-of-security/latest-security-news/wiper-malware-behind-sony-hack-illustrates-the-importance-of-risk-management.

19. Peter Elkind, *Inside the Hack of the Century*, FORTUNE (June 25, 2015, 6:00 AM), http://fortune.com/sony-hack-part-1.

20. *Id.*

21. Andrea Peterson, *Why It's So Hard to Calculate the Cost of the Sony Pictures Hack*, WASH. POST (Dec. 5, 2014), https://www.washingtonpost.com/news/the-switch/wp/2014/12/05/why-its-so-hard-to-calculate-the-cost-of-the-sony-pictures-hack.

22. *See, e.g.*, *id.*

23. GABRIEL SANCHEZ, SANS INST., CASE STUDY: CRITICAL CONTROLS THAT SONY SHOULD HAVE IMPLEMENTED 4–5 (2015), https://www.sans.org/reading-room/whitepapers/casestudies/case-study-critical-controls-sony-implemented-36022 ("Utilizing even a few of these Critical Controls, such as

The hack also came with concrete costs. The attack significantly reduced the value of some of Sony's most significant assets—its movies. Four unreleased Sony movies were leaked online.[24] Furthermore, in February 2015, Sony estimated that the costs of investigating and remediating the attack would be approximately $35 million.[25] Additionally, Sony faced class action litigation filed on behalf of approximately 437,000 individuals whose personal information was disclosed in the breach.[26] In 2016, a federal judge approved a settlement that included identity theft protection and legal fees.[27] The total costs of the settlement were estimated at $15 million.[28]

Beyond the harm to Sony and its employees, the hack had a tremendous impact on the U.S. government and its citizens. In December 2014, the U.S. government publicly stated that North Korea was behind the Sony attack as retaliation for Sony's planned release of *The Interview*, a fictional movie about an attempted assassination of Kim Jong Un.[29] Attributing a cyberattack to a nation–state is exceedingly rare, and the United States and other nations have not yet figured out how to respond to such attacks.[30] While cyberattacks that

malware defenses, monitoring, audit logs, encryption, controlled use of administrative credentials, and incident response could have provided the necessary implementations required to prevent a 90's hacker movie from turning into reality.").

24. Elkind, *supra* note 19.

25. Tim Hornyak, *Hack to Cost Sony $35 Million in IT Repairs*, NETWORK WORLD (Feb. 4, 2015, 12:25 AM), https://www.networkworld.com/article/2879814/data-center/sony-hack-cost-15-million-but-earnings-unaffected.

26. Annie Lowrey, *Sony's Very, Very Expensive Hack*, N.Y. MAG. (Dec. 16, 2014, 5:47 PM), http://nymag.com/daily/intelligencer/2014/12/sonys-very-very-expensive-hack.html.

27. Dominic Patten, *Sony Hack Class Action Settlement Gets Final Approval*, DEADLINE (Apr. 6, 2016, 10:36 AM), http://deadline.com/2016/04/sony-hack-lawsuit-settlement-approved-class-action-1201732882.

28. *Id.*

29. Ellen Nakashima, *U.S. Attributes Cyberattack on Sony to North Korea*, WASH. POST (Dec. 19, 2014), https://www.washingtonpost.com/world/national-security/us-attributes-sony-attack-to-north-korea/2014/12/19/fc3aec60-8790-11e4-a702-fa31ff4ae98e_story.html; *see also* Justin L. Koplow, *On Designation of North Korea as a State Sponsor of CyberTerrorism*, 18 SMU SCI. & TECH. L. REV. 405, 405–06 (2015) ("[S]everal recent incidents suggest a developing and growing trend of what seem to be ideologically motivated cyberattacks, intended to change the behavior of the attack targets or society and, in some cases, cause serious damage in the process. The 2014 hack of Sony Pictures Entertainment (Sony) is the most notorious example of this trend. From that attack, gallons of digital ink were spilled and consequences both serious and hilarious abounded. We learned that Channing Tatum sends emails IN ALL CAPS; at least one executive lost her job; viewing a terrible movie briefly became a defiant political act; reams of employee health information were made public, forming the basis of class action litigation; and sanctions were imposed upon North Korean entities via Executive Order.").

30. Lily Hay Newman, *Hacker Lexicon: What Is the Attribution Problem?*, WIRED (Dec. 24, 2016, 7:00 AM), https://www.wired.com/2016/12/hacker-lexicon-attribution-problem ("After months of news about Russian meddling in this year's US presidential election you're probably sick of speculation and ready for answers: What exactly did Russia do and why? It sounds simple enough, but a fundamental concept in cybersecurity and digital forensics is the fact that it is sometimes extremely difficult after a cyberattack to definitively name a perpetrator. Hackers have a lot of technical tools at their disposal to cover their tracks."); Bruce Schneier, *Hacker or Spy? In Today's Cyberattacks, Finding the Culprit Is a*

cause physical damage (such as an attack on a power grid) likely would be viewed as armed attacks that entitle the target to exercise self-defense under international law, mere attacks on data generally do not rise to the bar of an "armed attack."[31] Two weeks after the U.S. government attributed the hack to North Korea, President Obama issued an executive order that imposed sanctions against North Korean government agencies, organizations, and officials.[32] In a statement announcing the sanctions, the White House stated that the actions were in response to "North Korea's ongoing provocative, destabilizing, and repressive actions and policies, particularly its destructive and coercive cyber attack on Sony Pictures Entertainment."[33]

Despite the White House's forceful statements against North Korea's actions, the hack had a massive chilling effect on free speech. The hackers threatened physical violence at screenings of *The Interview*, causing Sony to cancel the initial theatrical release, a move that President Obama criticized as a "mistake"[34] because it allowed a dictator to "start imposing censorship here in the United States."[35] Sony soon scheduled a more limited theatrical release and also distributed the movie online and on-demand.[36] However, the damage from the hack endured and continued to chill speech in the entertainment industry.[37] In 2015, as Disney and Hearst attempted to create

Troubling Puzzle, CHRISTIAN SCI. MONITOR (Mar. 4, 2015), https://www.csmonitor.com/World/Passcode/Passcode-Voices/2015/0304/Hacker-or-spy-In-today-s-cyberattacks-finding-the-culprit-is-a-troubling-puzzle ("[W]e're living in a world where we can't easily tell the difference between a couple of guys in a basement apartment and the North Korean government with an estimated $10 billion military budget. And that ambiguity has profound implications for how countries will conduct foreign policy in the Internet age.").

31. Michael Schmitt, *International Law and Cyber Attacks: Sony v. North Korea*, JUST SECURITY (Dec. 17, 2014, 9:29 AM), https://www.justsecurity.org/18460/international-humanitarian-law-cyber-attacks-sony-v-north-korea ("The cyber operation against Sony involved the release of sensitive information and the destruction of data. In some cases, the loss of the data prevented the affected computers from rebooting properly. Albeit highly disruptive and costly, such effects are not at the level most experts would consider an armed attack.").

32. Dan Roberts, *Obama Imposes New Sanctions Against North Korea in Response to Sony Hack*, GUARDIAN (Jan. 2, 2015, 4:08 PM), https://www.theguardian.com/us-news/2015/jan/02/obama-imposes-sanctions-north-korea-sony-hack-the-interview.

33. Press Release, White House, Statement on the Executive Order Entitled "Imposing Additional Sanctions with Respect to North Korea" (Jan. 2, 2015), https://obamawhitehouse.archives.gov/the-press-office/2015/01/02/statement-press-secretary-executive-order-entitled-imposing-additional-s.

34. Tom Huddleston, Jr., *Movie Theaters to Screen 'The Interview' on Christmas Day*, FORTUNE (Dec. 23, 2014), http://fortune.com/2014/12/23/sony-screen-the-interview.

35. President Barack Obama, Remarks in Year-End Press Conference (Dec. 19, 2014), https://obamawhitehouse.archives.gov/the-press-office/2014/12/19/remarks-president-year-end-press-conference.

36. Huddleston, *supra* note 34.

37. Jessica E. Easterly, Note, *Terror in Tinseltown: Who Is Accountable When Hollywood Gets Hacked*, 66 SYRACUSE L. REV. 331, 337 (2016) ("With the threat of another release of confidential documents and potential terrorist attacks at the New York premiere of *The Interview*, Sony caved and decided to pull the movie from theaters. This decision was a catch-22 for Sony because if the movie was not

a cable news channel with Vice Media, Disney and Hearst reportedly requested a contractual provision that prohibited "any programming [that] impugns the reputation of a sovereign nation, or embarrasses Hearst and Disney in any way."[38] A report on the contractual clause described its "spirit" as standing for the principle that "if you renegades at Vice go off and do something that offends Kim Jong-un or any group of people, and we find ourselves damaged," Disney and Hearst would be able to sue for damages.[39]

The diversity of harms made Sony Pictures a particularly stark illustration of the effects of a cybersecurity attack. Before the attack on Sony, some of the highest-profile cybersecurity attacks involved the theft of credit card information at retailers, which caused potential harm for customers, banks, and retailers.[40] The Sony Pictures attack caused potential economic harm, but it went far beyond just that.[41] Stepping back, the Sony hack caused a wide range of harms to the United States, its companies, and its citizens. Among the most prominent harms were: (1) privacy harms to Sony employees; (2) embarrassment of Sony executives and celebrities; (3) reduced market value of leaked films; (4) internal operations slowdown at Sony; (5) harm to Sony's business reputation; (6) reduced public confidence in the security of electronic communications; (7) chilling effect on free speech and press; and (8) a symbolic victory of North Korean government over the United States.

---

pulled from theaters, they would be blamed for a terrorist attack (assuming the hackers carried through with their threats), but if the movie was pulled, Sony would be (and was) crucified for caving to terrorists' demands and diminishing the First Amendment." (footnote omitted)).

38. Sharon Waxman, *Vice, Disney at Impasse in TV Channel Talks Over 'Sony Hack' Clause*, WRAP (Jan. 19, 2015, 6:49 PM), http://www.thewrap.com/vice-disney-at-impasse-in-tv-channel-talks-over-sony-hack-clause-exclusive.

39. *Id.*

40. *See, e.g.*, Ahiza Garcia, *Target Settles for $39 Million Over Data Breach*, CNN (Dec. 2, 2015, 5:48 PM), http://money.cnn.com/2015/12/02/news/companies/target-data-breach-settlement/index.html ("The banks lost millions when they were forced to reimburse customers who lost money in the massive 2013 hack of Target's database. The banks, which service MasterCard, filed a class action lawsuit against Target after rejecting an earlier $19 million deal. MasterCard had tentatively approved that deal in April on behalf of its card issuers, but several of the banks rejected it."); Jonathan Stempel, *Home Depot Settles Consumer Lawsuit over Big 2014 Data Breach*, REUTERS (Mar. 8, 2016, 10:33 AM), http://www.reuters.com/article/us-home-depot-breach-settlement/home-depot-settles-consumer-lawsuit-over-big-2014-data-breach-idUSKCNoWA24Z ("Home Depot Inc[.] . . . agreed to pay at least $19.5 million to compensate U.S. consumers harmed by a 2014 data breach affecting more than 50 million cardholders. The home improvement retailer will set up a $13 million fund to reimburse shoppers for out-of-pocket losses, and spend at least $6.5 million to fund 1-1/2 years of cardholder identity protection services.").

41. *See* Andrea Peterson, *The Sony Pictures Hack, Explained*, WASH. POST (Dec. 18, 2014), https://www.washingtonpost.com/news/the-switch/wp/2014/12/18/the-sony-pictures-hack-explained ("While the news has been dominated by big retail hacks over the past year, the Sony Pictures cyberattack was much more disruptive: It knocked out computer systems at the company, and the fallout from the wholesale distribution of internal documents is far different from having to respond to the theft of credit card numbers.").

In other words, the attack on Sony Pictures created the perfect storm of harmful effects that worries cybersecurity professionals and policymakers.[42] These harms provide useful guidance as we develop the contours of cybersecurity law. Although every cybersecurity incident has a unique set of circumstances and fallout, the Sony attack provides among the broadest set of implications for the legal community to consider as it develops this new legal field.

Sony Pictures was not an anomaly. Multipronged cyberattacks, often originating from adversarial countries, threaten individual rights, U.S. security interests, and the economy as a whole. Less than two years later, hackers from another country—Russia—would launch cyberattacks on private and public infrastructure that would have dire effects on the United States.[43] Lawmakers and others who can shape cyber-policy should learn from such events to ensure that laws address these evolving threats.

III. DEFINING "CYBERSECURITY LAW"

The Sony incident—and similar cybersecurity challenges that companies and governments have faced—provide us with a roadmap for defining this new area of law. A clear definition of "cybersecurity law" is necessary for lawmakers, regulators, courts, and commentators to offer solutions to these ongoing threats. This Part offers some elements of the definition based on the experiences with incidents such as the attack on Sony Pictures. This Part concludes with a suggested comprehensive definition of "cybersecurity law."

To form the definition, we must answer five fundamental questions that examine the underlying values that should shape our cybersecurity laws: (1) What are we securing?; (2) Where and whom are we securing?; (3) How are we securing?; (4) When are we securing?; and (5) Why are we securing?

After addressing these five framing questions, this Article proposes a definition for "cybersecurity law" that takes into account the important considerations in the field of cybersecurity. This definition allows us to assess the current laws that are frequently associated with cybersecurity and explore the areas where they are lacking.

42. *See* Lawrence J. Trautman, *Cybersecurity: What About U.S. Policy?*, 2015 U. ILL. J.L. TECH. & POL'Y 341, 358 ("The North Korean cyber attack on Sony Pictures destroyed data and disabled thousands of computers, and exposed the personal information of Sony employees. And these attacks are hurting American companies and costing American jobs. So this is also a threat to America's economic security." (quoting President Barack Obama, Remarks at the Cybersecurity and Consumer Protection Summit (Feb. 13, 2015), https://obamawhitehouse.archives.gov/the-press-office/2015/02/13/remarks-president-cybersecurity-and-consumer-protection-summit)).

43. *See, e.g.*, 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.

A. WHAT ARE WE SECURING?

At the outset of any attempt to define "cybersecurity law," it is necessary to understand the intended subject matter. In other words, *what* should the law seek to secure? Based on the ongoing drumbeat of significant and damaging cybersecurity incidents[44] and the increased vulnerability due to the connection of everyday devices to the Internet,[45] I propose that "cybersecurity law" broadly seek to promote the confidentiality, integrity, and availability of information, systems, and networks.

Cybersecurity often is conflated, particularly in legal circles, with data security.[46] Although data security is an important part of cybersecurity, it is only one part. Cybersecurity focuses not only on the protection of data, but also on the systems and networks of the public and private sector. In other words, cybersecurity involves more than merely the protection of data.

Consider, for example, the 2016 Distributed Denial of Service ("DDOS") attack on Dyn, a relatively obscure but exceptionally important company that provides a large portion of the domain name system that directs traffic on the Internet.[47] A DDOS attack floods a targeted server with traffic from multiple sources, causing a slowdown in traffic or a complete shutdown.[48] Due to the DDOS attack on Dyn, Netflix, Twitter, and other popular online services were

44. DUSTIN SACHS, NAVIGANT CYBER THREAT INTELLIGENCE REPORT 2 (2017), https://www.navigant.com/-/media/www/site/insights/legal-technology/2017/cyberthreatintelligencereport_q12017.pdf ("As we turn to these challenges in 2017, it is noteworthy that the level and ferocity of attacks seems to continue unabated. From remote desktop hacking to national cyber armament, and the looming specter of another season of tax return-based identity theft, 2017 is shaping up to be another watershed year for cyber threats.").

45. *Id.* ("The increased reliance on industrial automation, drones, self-driving cars, and the continued expansion of connected-device technology, coupled with a shift in the global regulatory structure, all make 2017 a formative year in the progression of information security and cyber threats, both domestically and globally.").

46. Jason Fornicola, *Cybersecurity vs. Data Security: Government's Two-Pronged Challenge*, FED. NEWS RADIO (Oct. 7, 2015, 10:01 AM), https://federalnewsradio.com/sponsored-content/2015/10/cybersecurity-vs-data-security-governments-two-pronged-challenge ("Many organizations, agencies and the private sector spend much of their resources on cybersecurity. And with the recent data breaches at the Office of Personnel Management, Target, JP Morgan Chase and a host of other large organizations, are agencies and companies focusing on the wrong issues? If you look at recent legislation, it's focused on information security, whether it's the federal information security management act or the cyber information sharing protection act or a host of other bills. Then what is cybersecurity and how does it relate to data security?").

47. *See* Nicky Woolf, *DDoS Attack That Disrupted Internet Was Largest of Its Kind in History, Experts Say*, GUARDIAN (Oct. 26, 2016, 4:42 PM), https://www.theguardian.com/technology/2016/oct/26/ddos-attack-dyn-mirai-botnet. A Domain Name System is "[t]he Internet's system for converting alphabetic names into numeric IP addresses." *DNS*, PC MAG., https://www.pcmag.com/encyclopedia/term/41620/dns (last visited Dec. 21, 2017).

48. Woolf, *supra* note 47 ("The cause of the outage was a distributed denial of service (DDoS) attack, in which a network of computers infected with special malware, known as a 'botnet', are coordinated into bombarding a server with traffic until it collapses under the strain.").

unavailable for the majority of a day.[49] Although the attack resulted in some data being unavailable, it would not be characterized as a traditional data security compromise. Instead, it was an attack that compromised an entire network.[50] Laws focused exclusively on data—rather than networks and systems—will do little to prevent and remediate harms such as the Dyn attack.

To be sure, data security is a vital component of cybersecurity. For instance, the attack on Sony compromised a significant amount of the company's valuable data, including confidential emails and unreleased movies. That aspect of the attack attracted a great deal of publicity.[51] However, Sony also suffered great business harm due to the unavailability of its systems and networks.[52] The attack on Sony, in other words, was not *merely* an attack on the company's data security. It was a comprehensive attack on Sony's cybersecurity. The attack compromised more than just the confidentiality of Sony's information, though it certainly had that effect as well. The attack compromised the fundamental ability of Sony to carry out its routine business operations.

A focus on the security of systems and networks—and not just information—is necessary as physical devices are increasingly connected to the Internet. For instance, policymakers and regulators are understandably concerned about a cyberattack on a connected automobile that causes a highway crash, or a remote exploit of a factory's control systems that causes explosions, physical injury, and property damage.[53] By focusing exclusively on attacks on information, cybersecurity law would not address such threats to cyber-physical systems. Cybersecurity law should be flexible enough to address not only the incidents that already have occurred, but also potential future vectors of attack.

49. *Id.*

50. *Id.*

51. *See, e.g.*, Katie Richards, *The 5 Most Embarrassing Revelations From Sony's Sprawling Hack*, ADWEEK (Dec. 13, 2014), http://www.adweek.com/brand-marketing/5-most-embarrassing-revelations-sonys-sprawling-hack-161937 ("The true scope of a massive hacking attack against Sony Pictures remains unknown, but one thing is clear: Each new revelation seems to dig the studio only deeper into a public relations sinkhole.").

52. Amanda Hess, *Inside the Sony Hack*, SLATE (Nov. 22, 2015, 8:25 PM), http://www.slate.com/articles/technology/users/2015/11/sony_employees_on_the_hack_one_year_later.html ("The telephone directory vanished. Voicemail was offline. Computers became bricks. Internet access on the lot was shuttered. The cafeteria went cash-only. Contracts—and the templates those contracts were based on—disappeared. Sony's online database of stock footage was unsearchable. It was near impossible for Sony to communicate directly with its employees—much less ex-employees, who were also gravely affected by the hack—to inform them of what was even happening and what to do about it.").

53. Melissa Daniels, *Lawmakers Urge Study of Connected Cars, Possible Regs*, LAW360 (Jan. 25, 2017, 8:29 PM), https://www.law360.com/articles/884863/lawmakers-urge-study-of-connected-cars-possible-regs ("A bipartisan pair of congressmen want the National Highway Traffic Safety Administration to study connected cars and come up with regulations for automotive software, such as diagnostic and navigation systems, saying safeguards are needed against potential cybersecurity attacks.").

Therefore, when we develop the contours for cybersecurity law, we must develop a broader and more appropriate approach. The National Initiative for Cybersecurity Careers and Studies reflects such an approach, as its definition of "cybersecurity" is "[t]he activity or process, ability or capability, or state whereby information and communications systems and the information contained therein are protected from and/or defended against damage, unauthorized use or modification, or exploitation."[54] This definition captures the need to protect not only data, but also the systems on which data are stored and the networks on which data are transmitted. A definition of "cybersecurity law" that includes this important aspect will focus on the threats posed by cyberattacks.

We have established that cybersecurity law should focus not only on the security of information, but on systems and networks as well. However, the law does not provide much clarity as to what "security" means in the context of cybersecurity. Even though we know that we are securing information, networks, and systems, what do we mean by "securing"? Relatedly, how do we accomplish this task?

Cybersecurity professionals commonly think about security as covering three general categories of goals: (1) confidentiality; (2) integrity; and (3) availability, known in the industry as the "CIA Triad."[55] Confidentiality refers to the "the prevention of unauthorized disclosure of information."[56] Confidentiality often is associated with data breaches because attackers seek to obtain information without proper authorization. Integrity refers to "the guarantee that the message that is sent is the same as the message received and that the message is not altered in transit."[57] The defacement of a company's website, for example, is an example of a threat to data integrity. A threat to integrity also could refer to the modification of a business's financial records, as such a modification would cause internal chaos for the business's operations.[58] Availability refers to "the guarantee that information will be

54. *Glossary*, NAT'L INITIATIVE FOR CYBERSECURITY CAREERS & STUD. (Aug. 2, 2017), https://niccs.us-cert.gov/glossary.

55. Ashish Agarwal & Aparna Agarwal, *The Security Risks Associated with Cloud Computing*, 1 INT'L J. COMPUTER APPLICATIONS ENGINEERING SCI. (SPECIAL ISSUE ON CNS) 257, 257–58 (2011).

56. *Id.*

57. *Id.*

58. *See Worldwide Cyber Threats: Hearing Before the H. Permanent Select Comm. on Intelligence*, 114th Cong. 5 (2015) (statement of James R. Clapper, Director of National Intelligence), https://www.dni.gov/files/documents/HPSCI%2010%20Sept%20Cyber%20Hearing%20SFR.pdf ("Most of the public discussion regarding cyber threats has focused on the confidentiality and availability of information; cyber espionage undermines confidentiality, whereas denial-of-service operations and data-deletion attacks undermine availability. In the future, however, we might also see more cyber operations that will change or manipulate electronic information in order to compromise its integrity (i.e., accuracy and reliability) instead of deleting it or disrupting access to it. Decisionmaking by senior government officials (civilian and military), corporate executives, investors, or others will be impaired if they cannot trust the information they are receiving.").

available to the consumer in a timely and uninterrupted manner when it is needed regardless of [the] location of the user."[59] A DDOS attack that knocks a popular website offline, for example, is an attack on that site's availability.

The Sony Pictures attack threatened all three prongs of the CIA triad. The hackers compromised the confidentiality of employees' personal information as well as the company's highly sensitive business information. By altering the interface of the Sony Pictures internal computer systems, the attackers compromised the integrity of Sony's systems. The attack also harmed the availability of Sony's information and systems, as employees were unable to access the network.

Likewise, the reports of Russian interference in the 2016 U.S. elections demonstrate attempts to attack the entire CIA triad. The hack of Clinton campaign chairman John Podesta's emails was a classic compromise of confidentiality.[60] But Russia at least attempted to do more than access private emails. According to media reports, Russian hackers accessed voter databases and other elections systems in 39 states.[61] These attacks may have been attempts to compromise the integrity of U.S. voting data. Had the hackers knocked the voting systems offline on election day, the attacks would have compromised the availability of information systems and networks that are fundamental to U.S. democracy.

As Part IV of this Article explains, U.S. cybersecurity-related laws heavily focus on only one prong of the CIA Triad: confidentiality. This focus is because many of the statutes and regulations that intersect with cybersecurity are outgrowths of privacy law, which has a much more established field of jurisprudence and theory that has developed over more than a century.[62] The conflation of privacy and cybersecurity is understandable,[63] as many highly publicized cybersecurity incidents have involved breaches of sensitive information. While cybersecurity law should be concerned about preventing privacy violations, that should not be the unilateral focus of our approach to cybersecurity law. To be sure, we want to make sure that cybersecurity law

59. Agarwal & Agarwal, *supra* note 55, at 258.

60. *See, e.g.*, Tom O'Connor, *FBI Probe into Clinton Emails Prompted Offer of Cash, Citizenship for Confession, Russian Hacker Claims*, NEWSWEEK (May 11, 2017, 12:01 PM), http://www.newsweek.com/fbi-investigation-clinton-emails-russia-hack-607538.

61. *See, e.g.*, Michael Riley & Jordan Robertson, *Russian Cyber Hacks on U.S. Electoral System Far Wider Than Previously Known*, BLOOMBERG (June 13, 2017, 4:00 AM), https://www.bloomberg.com/news/articles/2017-06-13/russian-breach-of-39-states-threatens-future-u-s-elections.

62. *See* Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 193 (1890) (observing that the common law right to property "has grown to comprise every form of possession—intangible, as well as tangible").

63. *See* Bob Siegel, *What Is the Difference Between Privacy and Security?*, CSO (May 26, 2016, 5:24 AM), https://www.csoonline.com/article/3075023/privacy/the-difference-between-privacy-and-security.html ("Security provides protection for all types [of] information, in any form, so that the information's confidentiality, integrity, and availability are maintained. Privacy assures that personal information (and sometimes corporate confidential information as well) are collected, processed (used), protected and destroyed legally and fairly.").

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.

A focus on integrity and availability is particularly important in the Internet of Things era, as everyday devices, ranging from medical devices to kitchen appliances to automobiles, are connected to the Internet.[64] Imagine the chaos if hackers manage to disable thousands of pacemakers, or cause vehicles to accelerate to 100 miles per hours as they drive through Times Square. Such attacks have little to do with confidentiality of information, and instead involve the integrity and availability of systems and networks.

B. WHERE AND WHOM ARE WE SECURING?

So far, we have determined that cybersecurity law should promote the confidentiality, integrity, and availability of information, systems, and networks. We also must examine *which* information, systems, and networks should be protected under cybersecurity law. Should U.S. laws focus on bolstering the security of military and civilian government systems? Or should the laws apply equally rigorous requirements for private-sector cybersecurity? This confusion leads to both overlapping legal requirements and blind spots, caused partly by the application of criminal and international law principles to cyberspace.[65] The security of public infrastructure often will face quite different legal requirements than the security of private infrastructure. However, the policymakers should consider the security of both types of systems and networks comprehensively, and understand how the security (or lack thereof) of one affects the other.

The fundamental design of the Internet would make it impossible to effectively address cybersecurity exclusively through the information and infrastructure of the public sector. Government systems intertwine with

64. *See* FED. TRADE COMM'N, INTERNET OF THINGS: PRIVACY AND SECURITY IN A CONNECTED WORLD, at i (2015), https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf.

> The Internet of Things . . . refers to the ability of everyday objects to connect to the Internet and to send and receive data. It includes, for example, Internet-connected cameras that allow you to post pictures online with a single click; home automation systems that turn on your front porch light when you leave work; and bracelets that share with your friends how far you have biked or run during the day.

Id.

65. Susan W. Brenner, *Cyber-Threats and the Limits of Bureaucratic Control*, 14 MINN. J.L. SCI. & TECH. 137, 150–51 (2013) ("In cyberspace, states lose their monopoly on war and individuals lose their monopoly on crime and terrorism. This creates serious problems for countries like the United States, which rigidly bifurcate their threat response authority into (i) civilian (crime/terrorism) and (ii) military (war). The bifurcation is predicated on the assumption that response personnel can easily distinguish crime/terrorism from war." (footnotes omitted)).

private networks and rely on the infrastructure of telecommunications companies, cloud storage providers, and others in order to operate. In 2006, the Government Accountability Office recognized that one of the "key challenges" of securing Internet infrastructure was the diffuse control among the private and public sectors.[66] As described in Part IV of this Article, cybersecurity-related laws largely have not adapted in the decade since that report.

Often, it is difficult to isolate a target of an attack as private or public sector, just as it often is difficult to attribute an attack to a state or nonstate actor.[67] DDOS attacks, ransomware, and other common attack vectors can quickly disperse around the globe, and many do not discriminate between governments, companies, and individuals.[68] Accordingly, any effective cybersecurity law regime will seek to secure *both* the public sector and private sector. As seen after the Sony Pictures attack, even if the initial target is a private company that lacks strong links to the government, the fallout of an attack on that company can have significant ramifications for the federal government and international relations. Therefore, it would be short-sighted for cybersecurity law to focus exclusively on the public infrastructure and government information.

Accordingly, when policymakers develop cybersecurity laws, they should consider the security of both public and private infrastructure and information. As discussed in more detail in Part IV of this Article, some U.S. cybersecurity laws focus exclusively on certain sectors and do not consider how they operate in conjunction with laws that address cybersecurity of other sectors. To the greatest extent possible, cybersecurity law should operate

66. *See* GOV'T ACCOUNTABILITY OFFICE, GAO-06-672, INTERNET INFRASTRUCTURE: DHS FACES CHALLENGES IN DEVELOPING A JOINT PUBLIC/PRIVATE RECOVERY PLAN 37 (2006), http://www.gao.gov/assets/260/250483.pdf ("The diffuse control of the Internet makes planning for recovering from a disruption more challenging. The components of the Internet are not all governed by the same organization. Some components of the Internet are controlled by government organizations, while others are controlled by academic or research institutions. However, the vast majority of the Internet is owned and operated by the private sector. Each organization makes decisions to implement or not implement various standards based on issues such as security, cost, and ease of use.").

67. *See* JASON HEALEY, ATL. COUNCIL, BEYOND ATTRIBUTION: SEEKING NATIONAL RESPONSIBILITY FOR CYBER ATTACKS 1 (2012), http://www.atlanticcouncil.org/images/files/publication_pdfs/403/022212_ACUS_NatlResponsibilityCyber.PDF ("For more than two decades, cyber defenders, intelligence analysts, and policymakers have struggled to determine the source of the most damaging attacks. This 'attribution problem' will only become more critical as we move into a new era of cyber conflict with even more attacks ignored, encouraged, supported, or conducted by national governments.").

68. *The Backbone of the Internet Is Under Attack*, N.Y. POST (Oct. 21, 2016, 2:34 PM), http://nypost.com/2016/10/21/cyber-attacks-shutdown-twitter-spotify ("Cyberattacks targeting a little-known internet infrastructure company, Dyn, disrupted access to dozens of websites Friday, preventing some users from accessing PayPal, Twitter and Spotify. Dyn, whose customers include some of the world's most widely visited websites, said it did not know who was responsible for the outages that began in the Eastern United States, and then spread to other parts of the country and overseas. The outages were intermittent, making it difficult to identify all the victims.").

harmoniously across sectors. It is inevitable that highly sensitive information and systems—such as in the healthcare sector—may face more rigorous laws than in other areas, but those laws should not function in a black box.

C. HOW ARE WE SECURING?

We have determined that we want to secure the confidentiality, integrity, and availability of public and private information, systems, and networks. A difficult question—particularly in the context of lawmaking—is *how* to achieve those goals. This debate often appears to be a binary choice: coercive laws that deter inadequate cybersecurity versus cooperative laws that provide incentives for companies and government agencies to invest in cybersecurity.[69] I propose that cybersecurity law focus on both coercive *and* cooperative laws, provided that the regulations and incentives for both systems are aligned to achieve similar goals.

The debate over coercive or cooperative laws is not new to the U.S. legal system. For instance, environmental-law scholars for decades have debated the most appropriate way to encourage companies to adapt their business processes to minimize harm to the environment.[70] Advocates of the coercive approach to environmental regulation argue that companies seek to maximize profits, and therefore their "decisions regarding compliance are based on self-interest; businesses comply when the costs of noncompliance outweigh the benefits of noncompliance."[71]

A regulatory model based on coercion and deterrence assumes robust government oversight through "extensive government monitoring and

69. *Compare* Timothy F. Malloy, *Regulation, Compliance and the Firm*, 76 TEMP. L. REV. 451, 453–54 (2003) (stating that the coercive approach views "the firm as a rational profit-maximizer, obeying the law only when it is in the firm's best economic interest to do so. Thus, violations occur when the perceived benefits of noncompliance exceed the anticipated cost of sanctions. This view of the firm is consistent with deterrence theory, which regulators have historically relied upon in developing their enforcement programs. The rational profit-maximizer view typically leads to the use of traditional enforcement techniques; namely, extensive government monitoring and inspections coupled with penalties for observed violations." (footnotes omitted)), *with id.* at 454–55 ("In this view of the firm, the act of compliance is not driven by the threat of legal sanctions. Instead, compliance flows from the firm's drive to obey the law, sometimes called the 'compliance norm.' The compliance norm is fueled by the belief that legitimate regulation—regulation that is developed and implemented fairly—ought to be followed. Because the compliance norm relies upon the firm's capacity to monitor and control its own behavior independent of external government sanctions, in theory norm-based regulatory programs should elicit compliance even where the firm's activity is shielded from the regulator's gaze." (footnotes omitted)).

70. Robert L. Glicksman & Dietrich H. Earnhart, *Depiction of the Regulator-Regulated Entity Relationship in the Chemical Industry: Deterrence-Based vs. Cooperative Enforcement*, 31 WM. & MARY ENVTL. L. & POL'Y REV. 603, 612–13 (2007) ("Companies can save money by not purchasing, installing, and operating pollution control equipment and can avoid additional training for workers by failing to comply with environmental regulations.").

71. *Id.* at 612.

inspections coupled with penalties for observed violations."[72] The penalties for noncompliance, therefore, must be sufficiently severe to encourage companies to invest in compliance and, in many cases, forego potential revenue.[73]

Critics of the coercive approach in environmental regulation have developed an alternative model, based on cooperation and incentives. Under this model, the government's function is not "to accumulate evidence of violations for subsequent enforcement actions, but rather to provide advice to regulated entities as a means of facilitating compliance."[74] With this approach, companies are not only profit-maximizers, but also "institutions influenced by a mix of civic and social motives."[75] For example, an environmental inspector would suggest improvements rather than impose severe penalties.

The debate over regulation is not unique to environmental law. Policymakers and academics have long debated how to best regulate financial services,[76] consumer safety,[77] and other areas.[78] In most of these areas, the end

72. *Id.* (quoting Malloy, *supra* note 69, at 454).

73. *See id.* at 614 ("The essential task for enforcement agencies, therefore, is to make penalties high enough and the probability of detection great enough that it becomes economically irrational for regulated entities to violate the law. It is also necessary for regulated entities to perceive that there is a significant likelihood that the government will bring an enforcement action when a violation is detected." (footnote omitted)).

74. *Id.* at 616.

75. *Id.* at 617 ("This model postulates that corporations are generally inclined to comply with the law (although developing accurate measurements of such inclinations is problematic). According to some analysts of environmental regulation, corporations have internalized the general societal norms about environmental protection. If businesses are generally committed to compliance with their regulatory obligations even without a coercive enforcement presence, the imposition of sanctions in the event that noncompliance occurs is not only unnecessary, but may even be counterproductive." (footnotes omitted)).

76. *See* Saule T. Omarova, *Wall Street As Community of Fate: Toward Financial Industry Self-Regulation*, 159 U. PA. L. REV. 411, 416 (2011) ("Given the complexity and global nature of the modern financial market, any government's attempt to regulate it in a purely unilateral command-and-control manner will inevitably encounter the fundamental problem of regulatory arbitrage, whereby financial institutions find new ways to get around government rules, thus creating a never-ending spiral of rulemaking and rule evading. Only by enlisting the industry's active participation in the regulatory process can this vicious circle be broken. Thus, the lack of attention to self-regulation is an important omission in the debate on regulatory reform in the financial services sector." (footnote omitted)).

77. Hiroshi Sarumida, *Comparative Institutional Analysis of Product Safety Systems in the United States and Japan: Alternative Approaches to Create Incentives for Product Safety*, 29 CORNELL INT'L L.J. 79, 142 (1996) ("Judicial systems, political institutions, and market mechanisms in the United States and Japan have created incentive signals targeting various types of product risks. Different characteristics of these institutional mechanisms in both countries suggest alternative approaches to encourage manufacturers to improve product safety.").

78. Jennifer Gordon, *Regulating the Human Supply Chain*, 102 IOWA L. REV. 445, 450 (2017) ("[H]arms to migrant workers are not generated by anomalous bad actors, but instead are structural. They are the product of the global market for labor under current economic conditions, laws, and enforcement levels."); Christine Jolls et al., *A Behavioral Approach to Law and*

result is not a binary choice. Legal regimes that apply to specific industries or sectors contain both coercive and cooperative elements.[79]

Cybersecurity law should contain a mix of penalty-based regulatory deterrence along with cooperation and incentives. A unilateral focus on coercion through regulation would be misguided, as there are many opportunities for cooperative cybersecurity law. As described above, cyberspace is a combination of public *and* private infrastructure. A threat to a company's cybersecurity can harm the government, and vice versa. Unlike other regulatory areas, regulators cannot achieve an ideal level of cybersecurity exclusively through the actions (voluntary or otherwise) of the private sector. Although a company's adoption of cybersecurity measures could help to reduce the likelihood of a successful cybersecurity incident, the ultimate chances of a successful attack depend on many other factors, including law enforcement's ability to deter hackers, the security of the company's service providers, and whether the government and companies can quickly communicate with each other about cybersecurity threats and defensive measures. Accordingly, for cybersecurity law to succeed, it must foster effective collaboration between the public and private sectors. As I describe below, we have made some strides toward that goal, primarily with the Cybersecurity Act of 2015. That statute takes the first significant steps to encourage the private sector and federal government to work together to identify and defend against cybersecurity threats. However, the vast majority of the laws broadly considered to be related to cybersecurity are punitive, and they do little to actually encourage investments in cybersecurity.

The U.S. legal system should continue to penalize behavior that degrades our nation's cybersecurity. The regulations, however, should have the ultimate effect of *encouraging* companies to invest in cybersecurity. Consider the Sony Pictures data breach. Three years earlier, in 2011, Sony's Play Station network experienced one of the largest data breaches in world history when tens of millions of customers' accounts (including credit card data) were compromised by hackers.[80] The company faced costly class action litigation and regulatory inquiries, and it reported that through the end of 2012, the breach cost the company $171 million.[81] Despite those regulatory and litigation costs—which are far higher than those associated with an average

Economics, 50 STAN. L. REV. 1471, 1544 (1998) ("We also emphasize that government intervention need not come in highly coercive forms; perhaps distortions in people's decisionmaking can be overcome by information campaigns falling well short of coercion.").

79. *See infra* Part III.C.

80. Liana B. Baker & Jim Finkle, *Sony PlayStation Suffers Massive Data Breach*, REUTERS (Apr. 26, 2011, 3:54 PM), http://www.reuters.com/article/us-sony-stoldendata/sony-playstation-suffers-massive-data-breach-idUSTRE73P6WB20110426.

81. John Gaudiosi, *Why Sony Didn't Learn from Its 2011 Hack*, FORTUNE (Dec. 24, 2014), http://fortune.com/2014/12/24/why-sony-didnt-learn-from-its-2011-hack.

cybersecurity incident[82]—Sony did not sufficiently change its organizational structure or invest in cybersecurity measures to prevent the Sony Pictures attack three years later.[83] Of course, Sony's failure to properly secure its networks does not mean that all companies would react similarly to the threat of significant fines and litigation costs. However, it demonstrates that for some companies, regulatory and litigation penalties alone will not deter bad behavior.

The questionable efficacy of coercive cybersecurity regulation is traceable, in part, to the relatively low costs of penalties for large companies. Benjamin Dean of Columbia University's School of International and Public Affairs analyzed the breaches at Sony Pictures, Target, and Home Depot, concluding that the breaches cost less than one percent of the companies' annual revenues.[84] This suggests that fines, court awards, and other expenses would need to be significantly higher to encourage corporate executives to invest in cybersecurity, even at the expense of other business units that might actually generate more revenues, such as marketing. Moreover, Dean notes, even if companies suffer significant expenses due to data breaches and other cybersecurity incidents, they often can be at least partially reimbursed by insurance, or they can write off those expenses.[85] This moral hazard, he reasoned, means that it "does not make economic sense for companies like Home Depot to make large investments in information security."[86] The cybersecurity vulnerabilities of individual companies—as seen in recent attacks on Equifax, Dyn, Target, and Ashley Madison—pose a significant risk to individuals and, in some cases, national interests. However, our legal system has not yet created adequate incentives for individual companies to take the necessary—and sometimes costly—steps to reduce the likelihood of cybersecurity attacks.

To create an incentive for greater cybersecurity investments, the government could raise the costs of data breaches to such a high level that even large companies would go out of business if they suffered a large data breach or other attack. The government could accomplish this punitive goal by imposing astoundingly high fines on companies that suffered from cybersecurity incidents, or by allowing plaintiffs to recover large damages in

82. *See* PONEMON INST., 2016 COST OF DATA BREACH STUDY: GLOBAL ANALYSIS 1 (2016), https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=SEL03094WWEN ("[T]he average total cost of a data breach . . . increased from $3.79 to $4 million.").

83. Gaudiosi, *supra* note 81 ("But there's one major factor that prevented Sony from better using those 2011 lessons in 2014: organizational structure. The company has long had a reputation for operating in silos, says Michael Pachter, a video game analyst at Wedbush Securities, and no silo is more isolated than Sony Pictures Entertainment.").

84. Benjamin Dean, *Why Companies Have Little Incentive to Invest in Cybersecurity*, CONVERSATION (Mar. 4, 2015, 2:26 PM), http://theconversation.com/why-companies-have-little-incentive-to-invest-in-cybersecurity-37570.

85. *Id.*

86. *Id.*

class action lawsuits. However, this strategy would be short-sighted for a few reasons. First, even companies that invest heavily in cybersecurity cannot anticipate every future vector of attack. A hyper-regulatory environment for cybersecurity likely would threaten to penalize even the companies that attempted to make adequate investments in safeguards. Second, and more practically, it is politically unlikely that Congress or state legislatures would impose fines so high that would threaten to put companies out of business.

That is not to say that cybersecurity should be a regulation-free zone. Coercion can play an important and necessary role in cybersecurity law. However, coercive measures should encourage the most effective safeguards, and these measures should be fairly imposed. Most importantly, coercive cybersecurity measures should be used in conjunction with cooperative laws.

Cooperation is particularly important for cybersecurity law, as compared to other business laws, because companies' goals often—but not always—are aligned with those of the government. It would be absurd for a rational Chief Executive Officer to be entirely indifferent to a cyberattack that cripples the company's operations for weeks. For instance, it is safe to say that both the U.S. government and Sony Pictures ultimately want to prevent another such attack. It is in the national interests and Sony's corporate interests to avoid another high-profile embarrassment at the hands of another country. In contrast, corporate and government interests are not necessarily aligned for environmental law. The federal government's goal may be to reduce pollution and negative impacts on the environment, while an automaker's goal may be to efficiently produce cars and maximize value to shareholders. Accordingly, there is far more room for cooperation with cybersecurity than with other areas. When we discuss cybersecurity law, we should consider *both* cooperation and coercion, and determine the appropriate blend that maximizes effective cybersecurity protections for both the public and private sector.

The coercive and cooperative cybersecurity laws must be harmonious. For instance, if the government determines that medical devices are particularly vulnerable to attacks, it could take a multipronged approach. First, the government could provide companies with the technical guidance to adopt adequate safeguards for the devices, as the National Institute of Standards and Technology ("NIST") often does by developing many cybersecurity controls.[87] Second, the government could create tax incentives for device-makers to invest in the technology and staff necessary to implement the controls. Third, the Food and Drug Administration ("FDA") could refuse to approve new devices that have not incorporated these controls into new products. Fourth, the FDA could impose heavy fines on companies that do not maintain these safeguards and fix vulnerabilities in existing devices. The

87. *See generally* U.S. DEP'T OF COMMERCE, NIST SPECIAL PUBLICATION 800-171, PROTECTING CONTROLLED UNCLASSIFIED INFORMATION IN NONFEDERAL SYSTEMS AND ORGANIZATIONS (2016), http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-171r1.pdf.

government need not choose only one of these options. Rather, all four approaches could achieve a common goal.

In short, a well-conceived legal framework will include incentives and penalties, and ensure that those policies achieve a common goal of improving cybersecurity. A legal system that consists entirely of coercion or entirely of cooperation likely will have limited success. The challenge for policymakers is to determine how to use a combination of penalties and incentives to most effectively encourage companies to adopt safeguards.

D. WHEN ARE WE SECURING?

By asking "when are we securing?," we must assess whether cybersecurity laws should focus on events that already have occurred, or if they should attempt to build resilience and defenses to prevent the attacks from occurring in the future.

To the greatest extent possible, cybersecurity law should be forward-looking. Cybersecurity law should prevent cybersecurity incidents from ever occurring, and if incidents do occur, cybersecurity law should help companies and government recover as quickly as possible and prevent future harmful events.

This element of the definition sounds obvious, but many of our laws are backward-looking. They require companies and regulators to litigate the minute details of incidents that already have occurred. In some cases, such retrospection may be valuable, as it can help companies and governments avoid repeating past mistakes. However, the ultimate focus always should be on preventing additional attacks and losses from occurring in the future.

The necessity of a forward-looking component of cybersecurity law is most apparent in any discussion of cyber-resilience, an increasing focus of cybersecurity professionals.[88] In 2013, President Obama issued Presidential Policy Directive 21, which encouraged the cybersecurity of critical infrastructure, such as the electric grid.[89] The Directive defines "resilience" as "the ability to prepare for and adapt to changing conditions and withstand and recover rapidly from disruptions," and it states that "[r]esilience includes the ability to withstand and recover from deliberate attacks, accidents, or naturally occurring threats or incidents."[90] The DHS has stated that resilience

88. *See* Daniel Dobrygowski, *Cyber Resilience: Everything You (Really) Need to Know*, WORLD ECON. F. (July 8, 2016), https://www.weforum.org/agenda/2016/07/cyber-resilience-what-to-know ("There is a multitude of ways in which an organization or society can be considered resilient, but a common denominator is the inclusion of a deep understanding of risk in strategic planning. For cyber risk, this means going beyond information-technology planning and making risk evaluation a normal part of strategy. Normalization is key. Cyber risk should be viewed just like any other risk that an organization must contend with in order to fulfil its goals.").

89. Press Release, White House, Presidential Policy Directive—Critical Infrastructure Security and Resilience (Feb. 12, 2013), https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil.

90. *Id.*

measures include business continuity plans, back-up power generators, and durable building materials.[91] This growing—and entirely justified—focus on resilience requires cybersecurity law to be forward-looking and consider not only how to prevent cybersecurity incidents from occurring (either through coercion or cooperation), but also how to recover from cybersecurity incidents once they have occurred.

This is not to say that cybersecurity laws should not address cybersecurity incidents that already have occurred. Companies that have been particularly negligent or reckless with their cybersecurity safeguards should expect to face consequences, such as regulatory investigations, fines, and lawsuits. Large fines and judgments could set an example for other companies and motivate them to invest in stronger cybersecurity safeguards. But the ultimate goal of penalties for past cybersecurity incidents should be deterrence of future events.

E. WHY ARE WE SECURING?

To fully define the scope of cybersecurity law, we must fully articulate our ultimate goals. The government should not impose regulations or make substantial investments until there is a more thorough understanding of why it is doing so.

The Sony Pictures attack caused great harm and embarrassment to individuals by allowing egregious privacy violations. The cyberattack also damaged Sony's business interests by exposing its confidential business information and significantly reducing the value of its movies. Finally, the incident threatened U.S. national security and further strained the U.S. government's relationship with North Korea. In short, the Sony Pictures attack (and others like it) highlight three distinct types of harm that cybersecurity law should seek to provide: (1) harm to individuals; (2) harm to business interests; and (3) harm to national security.

The first reason to enact cybersecurity laws is to prevent and mitigate harm to individuals. This harm often involves privacy violations,[92] such as the disclosure of the email messages of Sony executives and the personal information of Sony employees. Such disclosures are highly embarrassing and can have dramatic effects on individuals' lives. Courts and legislators often focus on the financial harm to individuals—such as the consequences of

91. *What is Security and Resilience?*, DEP'T HOMELAND SECURITY, https://www.dhs.gov/what-security-and-resilience (last visited Dec. 21, 2017).

92. *See* Warren & Brandeis, *supra* note 62, at 213 ("We must therefore conclude that the rights, so protected, whatever their exact nature, are not rights arising from contract or from special trust, but are rights as against the world; and, as above stated, the principle which has been applied to protect these rights is in reality not the principle of private property, unless that word be used in an extended and unusual sense. The principle which protects personal writings and any other productions of the intellect or of the emotions, is the right to privacy, and the law has no new principle to formulate when it extends this protection to the personal appearance, sayings, acts, and to personal relation, domestic or otherwise.").

identity theft—caused by data breaches. Indeed, in some consumer lawsuits against companies that have experienced data breaches, courts have refused to find that the plaintiffs have Article III standing unless the plaintiffs demonstrate that they have actually suffered identity theft as a result of the breach.[93] However, cybersecurity law—both statutes and court rulings—should attempt to prevent not only identity theft and other financial harm; cybersecurity law should address all potential harm to individuals caused by cybersecurity incidents. Daniel J. Solove and Danielle Keats Citron recently articulated this wide spectrum of harms by making a compelling case for courts to recognize the intangible harms of data breaches, such as increased anxiety among consumers:

> The harm from an increased risk of identity theft is akin to the risk of contracting a chronic disease. The risk of a data breach is ongoing. Data breach notification letters explicitly inform people that there is a risk of identity theft. Credit monitoring services are offered for one or two years, signaling to plaintiffs an increased risk of theft for that time period. When a person has a reasonable belief that her credit identity is in jeopardy, she is rightly afraid that her creditworthiness is out of her hands.[94]

The concern about anxiety-related harms to individuals could be seen after the 2015 data breach of Ashley Madison, a site that allowed users to seek extramarital affairs.[95] Despite the lack of concrete financial harm, the public disclosure of the names of Ashley Madison customers had far-reaching effects, including job resignations and suicides.[96]

93. *See, e.g.*, Reilly v. Ceridian Corp., 664 F.3d 38, 43 (3d Cir. 2011) ("[W]e cannot now describe how Appellants will be injured in this case without beginning our explanation with the word 'if': *if* the hacker read, copied, and understood the hacked information, and *if* the hacker attempts to use the information, and *if* he does so successfully, only then will Appellants have suffered an injury.").

94. Daniel J. Solove & Danielle Keats Citron, *Risk and Anxiety: A Theory of Data Breach Harms*, 96 TEX. L. REV. (forthcoming 2017) (manuscript at 26), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2885638.

95. *See* Robert Hackett, *What to Know About the Ashley Madison Hack*, FORTUNE (Aug. 26, 2015), http://fortune.com/2015/08/26/ashley-madison-hack ("The Ashley Madison hackers have posted personal information like e-mail addresses and account details from 32 million of the site's members. The group has claimed two motivations: First, they've criticized Ashley Madison's core mission of arranging affairs between married individuals. Second, they've attacked Ashley Madison's business practices, in particular its requirement that users pay $19 for the privilege of deleting all their data from the site (but, as it turns out, not all data was scrubbed).").

96. Tom Lamont, *Life After the Ashley Madison Affair*, GUARDIAN (Feb. 27, 2016, 7:05 PM), https://www.theguardian.com/technology/2016/feb/28/what-happened-after-ashley-madison-was-hacked ("Moral crusaders, operating with impunity, began to shame and squeeze the exposed. In Alabama editors at a newspaper decided to print in its pages all the names of people from the region who appeared on Ashley Madison's database. After some high-profile resignations all around North America, people wondered if there might not be a risk of more tragic repercussions. Brian Krebs, with some prescience, wrote a blog advising sensitivity: 'There's

The second reason to enact cybersecurity laws is to prevent economic harm to companies. On average, a data breach costs a company approximately $4 million, and the cost per stolen record is approximately $158, according to a recent report by the Ponemon Institute for IBM.[97] According to the report, a U.S. company has a 26% chance of experiencing a breach within 24 months of at least 10,000 records.[98] On aggregate, cybersecurity incidents take a significant economic toll. A recent study estimated that the aggregate cost of data breaches will exceed $2 trillion in 2019.[99] Cybersecurity law should attempt to reduce these negative impacts both on individual companies and the economy as a whole.

Finally, cybersecurity law must incorporate the national security interests of the United States. In the Sony incident, these concerns came to the forefront when the United States attributed the attack to North Korea and imposed sanctions, at the time an unprecedented move after a cyberattack. Similarly, Russia's interference in the 2016 U.S. election, via cyberattacks, threatened to fundamentally undercut the confidence and legitimacy of the U.S. democratic system. Even if the attacks target entirely private infrastructure—such as the email system of a political party—the consequences for the public and national security can be far-reaching.

Moreover, attacks on critical infrastructure—even if it is owned and operated by the private sector—can severely harm national security. President Obama recognized this danger in Presidential Policy Directive 21, writing of the need "to strengthen and maintain secure, functioning, and resilient critical infrastructure—including assets, networks, and systems—that are vital to public confidence and the Nation's safety, prosperity, and well-being."[100] To date, the United States has not suffered a devastating cyberattack on critical infrastructure that has caused significant physical damage, but serious critical infrastructure attacks have occurred in other countries. For instance, in 2007, Estonia, a small nation that is highly dependent on the Internet, suffered a massive economic slowdown after its cyber-infrastructure was hit with massive denial-of-service attacks.[101] In 2015, Ukraine suffered a

a very real chance that people are going to overreact,' he wrote. 'I wouldn't be surprised if we saw people taking their lives because of this.' A small number of suicides were reported, a priest in Louisiana among them.").

97. PONEMON INST., *supra* note 82, at 1.

98. *Id.* at 1, 21.

99. Steve Morgan, *Cyber Crime Costs Projected to Reach $2 Trillion by 2019*, FORBES (Jan. 17, 2016, 11:01 AM), https://www.forbes.com/sites/stevemorgan/2016/01/17/cyber-crime-costs-projected-to-reach-2-trillion-by-2019 (citing Press Release, Juniper Research, Cybercrime Will Cost Businesses Over $2 Trillion by 2019 (May 12, 2015), https://www.juniperresearch.com/press/press-releases/cybercrime-cost-businesses-over-2trillion).

100. Press Release, White House, *supra* note 89.

101. *See A Look at Estonia's Cyber Attack in 2007*, NBC NEWS (July 8, 2009, 2:24 PM), http://www.nbcnews.com/id/31801246/ns/technology_and_science-security/t/look-estonias-cyber-attack ("In April and May 2007, hackers unleashed a wave of cyber attacks that crippled dozens of government

cyberattack that caused blackouts for more than 80,000 people for several hours.[102] U.S. cyber officials have reported a rapid increase in the number of attacks on critical infrastructure, such as the industrial control systems of utilities.[103] Such attacks not only threaten economic and business interests; they can cause injuries, death, and national unrest. Accordingly, national security must be among the top considerations of cybersecurity law.

F. A PROPOSED DEFINITION OF "CYBERSECURITY LAW"

Factoring in all of these considerations, we can develop a broad and flexible definition that provides the general parameters and scope of cybersecurity law. By providing this definition, this Article does not intend to suggest that cybersecurity law should be limited to a particular set of policy prerogatives. Rather, this Article identifies areas that should be considered when we develop and refine laws that address cybersecurity:

> 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.

IV. ASSESSING CURRENT CYBERSECURITY LAWS

The United States has very few laws that mention cybersecurity by name. The lack of explicit references to cybersecurity is understandable, as "cybersecurity" is a relatively new term. Indeed, the first time that a published U.S. court opinion even used the word "cybersecurity" was in a footnote to a 2007 Seventh Circuit opinion.[104] However, there are a number of U.S. state and federal statutes, regulations, and court opinions regarding data security, hacking, and related issues that address some aspects associated with cybersecurity law.

In this Part, I apply the definition of "cybersecurity law" from Part III.F to the current U.S. framework of cybersecurity law to assess which parts of the definition the law addresses and which parts the law overlooks. In short, the

and corporate sites in Estonia, one of Europe's most wired countries. Estonian authorities traced the so-called denial of service attacks to Russia, and suggested they had been orchestrated by the Kremlin—a charge Moscow denied.").

102. Katie Bo Williams, *US Assisting Ukraine in Cyberattack Investigation*, HILL (Jan. 12, 2016, 3:38 PM), http://thehill.com/policy/cybersecurity/265597-us-assisting-ukraine-in-cyberattack-investigation ("The attackers also . . . launched a DDoS attack on the power company's customer service center, flooding it with phony calls to prevent customers from reporting the outages.").

103. Cory Bennett, *Critical Infrastructure Cyberattacks Rising, Says US Official*, HILL (Jan. 13, 2016, 2:19 PM), http://thehill.com/policy/cybersecurity/265753-critical-infrastructure-cyberattacks-rising-says-us-official ("The ICS-CERT said in its alert that it found a variant of the malware believed to have been used [in the] Ukraine attack in some U.S. critical infrastructure systems.").

104. *See* Pisciotta v. Old Nat'l Bancorp, 499 F.3d 629, 638 n.10 (7th Cir. 2007).

existing cybersecurity framework focuses largely on protecting the confidentiality of information for the purposes of protecting individual privacy. However, the laws could be improved to focus more other aspects, including: (1) integrity and availability; (2) protecting systems and networks; and (3) promoting economic and national security interests. Moreover, cybersecurity law could benefit from a more forward-looking perspective with the goal of preventing future incidents, rather than the current focus on penalizing companies for failing to safeguard against previous attacks.

Of course, this Article does not address every federal and state statute and common law claim that might relate to cybersecurity. Rather, I have focused on six categories of U.S. laws that are commonly associated with cybersecurity: (1) data security statutes; (2) data breach-notification statutes; (3) data security litigation through common law and statutory claims; (4) computer hacking laws; (5) electronic surveillance laws; and (6) the Cybersecurity Act of 2015.

A. DATA SECURITY STATUTES

In the United States, there are three general types of statutes (and, in some cases, accompanying regulations) that set requirements for data security, either explicitly or implicitly: (1) Section 5 of the Federal Trade Commission Act; (2) industry-specific federal data security laws, such as the Gramm–Leach–Bliley Act and the Health Insurance Portability and Accountability Act; and (3) state data security laws.

The Federal Trade Commission ("FTC") is the federal agency most closely associated with data security regulation. The FTC brings enforcement actions against companies that either (1) failed to enact adequate data security safeguards or (2) misrepresented their data security in privacy policies or other statements to consumers.[105] No statute explicitly provides the FTC with data security enforcement authority. Rather, the FTC claims the ability to bring data security cases under Section 5 of the Federal Trade Commission Act, which prohibits "unfair or deceptive acts or practices in or affecting commerce."[106] Section 5 states that an act may be considered "unfair" only if it "causes or is likely to cause substantial injury to consumers which is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition."[107] Although this provides some guidance, it does not specifically address the types of data security shortcomings that would cause substantial injury, or the

105. *See* Woodrow Hartzog & Daniel J. Solove, *The Scope and Potential of FTC Data Protection*, 83 GEO. WASH. L. REV. 2230, 2235 (2015) ("The FTC began its foray into privacy and data security by focusing on promises companies voluntarily made in their privacy policies. When companies later failed to live up to these promises, the FTC claimed that this was a deceptive trade practice." (footnote omitted)).

106. 15 U.S.C. § 45(a)(1) (2012).

107. *Id.* § 45(n).

magnitude of benefits necessary to outweigh a harmful lack of data security safeguards. The FTC has not issued formal regulations that explain how this century-old statute applies to data security, though it has issued informal guidance based on the dozens of data security actions it has brought under Section 5.[108] The FTC typically brings data security under the "deception" prong of Section 5 if a company has misrepresented its data security practices.[109] The Commission's data security authority under the "unfairness" prong has been more controversial and susceptible to legal challenges. In 2015, the United States Court of Appeals for the Third Circuit concluded that the "unfairness" prong of Section 5 provides the FTC with sufficient authority to bring enforcement actions against companies that failed to properly safeguard personal data.[110] The FTC has brought Section 5 actions against companies for failing to use adequate encryption for medical records,[111] neglecting to supervise service providers who handled sensitive information,[112] and failing to adequately train employees on data security.[113]

In addition, about a dozen states have passed statutes that specifically address corporate data security. Most of these laws—including the statutes in Arkansas,[114] California,[115] Connecticut,[116] Florida,[117] Indiana,[118] Maryland,[119] and Utah[120]—lack specificity and merely require companies to adopt "reasonable" data security plans. Oregon's data security law provides more specific guidance for reasonable security safeguards, such as conducting risk assessments, training employees, and regularly testing security controls.[121] Rhode Island requires companies to have reasonable security programs that

108. FED. TRADE COMM'N, START WITH SECURITY: A GUIDE FOR BUSINESS 1 (2015), https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf.

109. *See, e.g.*, Complaint at 3–5, *In re* Upromise, Inc., FTC File No. 102-3116, No. C-4351 (F.T.C. Mar. 27, 2012), 2012 WL 1225058.

110. FTC v. Wyndham Worldwide Corp., 799 F.3d 236, 245 (3d Cir. 2015) ("A company does not act equitably when it publishes a privacy policy to attract customers who are concerned about data privacy, fails to make good on that promise by investing inadequate resources in cybersecurity, exposes its unsuspecting customers to substantial financial injury, and retains the profits of their business.").

111. Complaint at 4, *In re* Henry Schein Practice Sols., Inc., FTC File No. 142-3161, No. C-4575 (F.T.C. May 20, 2016), 2016 WL 160609.

112. Complaint at 3–4, *In re* GMR Transcription Servs., Inc., FTC File No. 122-3095, No. C-4482 (F.T.C. Feb. 3, 2014), 2014 WL 492352.

113. Complaint at 2, *In re* Franklin's Budget Car Sales, Inc., File No. 102-3094, No. C-4371 (F.T.C. Oct. 3, 2012), 2012 WL 5375157.

114. ARK. CODE ANN. § 4-110-104(b) (2011).

115. CAL. CIV. CODE § 1798.81.5(b)–(c) (West 2005).

116. *See* 2008 Conn. Acts 611 (Reg. Sess.).

117. FLA. STAT. § 501.171(2) (2016).

118. IND. CODE ANN. § 24-4.9-3-3.5(b) (West 2015).

119. MD. CODE ANN., COM. LAW § 14-3503(a) (LexisNexis 2013).

120. UTAH CODE ANN. § 13-44-201(1)(a) (LexisNexis 2013).

121. OR. REV. STAT. ANN. § 646A.622 (West 2011).

are appropriate to their size, the nature of the information they handle, and the purpose of the information collection.[122] Nevada requires companies to use encryption in certain circumstances and to follow special data security standards for payment-card data.[123] Massachusetts has perhaps the most detailed data security regulations, requiring companies to take specific steps to assess security risks, train employees, oversee service providers, and implement other safeguards.[124]

Financial institutions face more specific data security requirements. In 1999, Congress passed the Gramm–Leach–Bliley Act, which, in addition to overhauling U.S. financial regulation, required that financial regulators mandate that their regulated institutions adopt "administrative, technical, and physical safeguards" for the security of "nonpublic personal information."[125] Financial regulators have taken various approaches to implementing this requirement. For instance, the Interagency Guidelines—which the Office of Comptroller of the Currency, Federal Reserve Board, Federal Deposit Insurance Corporation, and Office of Thrift Supervision jointly adopted—require that regulated institutions take steps such as involving the board of directors in the development of security programs, conducting risk assessments, testing security controls, and overseeing service providers' information security.[126]

Similarly, HIPAA requires health plans, healthcare clearinghouses, healthcare providers, and their business associates to adopt "administrative, technical, and physical safeguards" to protect individually identifiable health information.[127] Among the required safeguards are designating an information "security official,"[128] limiting access to physical facilities where protected health information is stored,[129] and maintaining activity logs of systems.[130]

The data security statutes also focus primarily on private-sector data security. Security of the federal government's information systems is governed by the Federal Information Security Management Act ("FISMA"),[131] which charges the White House's Office of Management and Budget, Department of Homeland Security, and National Institute of Standards and Technology

122. 11 R.I. GEN. LAWS ANN. § 11-49.3-2(a) (West 2006).

123. NEV. REV. STAT. § 603A.215 (2015).

124. 201 MASS. CODE REGS. 17.03 (2009).

125. Gramm–Leach–Bliley Act of 1999 § 501, 15 U.S.C. § 6801 (2012).

126. Interagency Guidelines Establishing Information Security Standards, 12 C.F.R. § 208 app. D–2 (2016).

127. Health Insurance Portability and Accountability Act of 1996 § 1173, 42 U.S.C. § 1320d-2(d)(2) (2012); *see also* 45 C.F.R. §§ 164.302–.318 (2016) (outlining the Department of Health and Human Services' security-standard regulations authorized by HIPAA).

128. 45 C.F.R. § 164.308(a)(2).

129. *Id.* § 164.310(a).

130. *Id.* § 164.312(b).

131. 44 U.S.C. §§ 3541–49 (2012).

with setting and enforcing information security standards.[132] These standards apply not only to federal agencies, but also to their contractors.[133] The private-sector data security standards are not aligned with the FISMA information security requirements for the public sector.

The data security laws are largely punitive, carrying the threat of large fines, consent decrees, or lawsuits. While coercive laws play some role in cybersecurity—just as they do in other areas such as environmental regulation—the laws also should provide at least for some degree of cooperation between the government and private sector, as the interests often are aligned.

B. DATA BREACH-NOTIFICATION STATUTES

Forty-eight states and the District of Columbia require companies to notify customers, regulators, and credit bureaus of data breaches.[134] Unfortunately, complying with the laws is not entirely intuitive, as the requirements for the notification are not uniform.

Each notification law requires notice only if an unauthorized party has acquired certain types of customer information. Typically, breach-notification laws require reporting if there has been unauthorized disclosure of an individual's name along with a Social Security number, driver's license or state identification number, or financial account number and access code.[135] However, some states have added categories of information that trigger a notification requirement. North Dakota, for instance, also requires notification of the disclosure of a date of birth, mother's maiden name, and other information.[136] Moreover, some statutes only require notification if the company determines that the breach poses a reasonable likelihood of harm to consumers, while others require notification regardless of the risk of harm.[137]

Because state breach-notification laws apply based on the residency of the 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.[138] This can prove to be complex and time-consuming, particularly for

132. *Id.* § 3543; 40 U.S.C. § 11331(b) (2012).

133. 44 U.S.C. § 3543.

134. For a list of all data breach notice statutes, see *Security Breach Notification Laws*, NAT'L CONF. ST. LEGISLATURES (Apr. 12, 2017), http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx.

135. *See, e.g.*, MINN. STAT. ANN. § 325E.61 (West 2011).

136. N.D. CENT. CODE §§ 51-30-01 to -03 (2007).

137. *See* JEFF KOSSEFF, CYBERSECURITY LAW 39 (2017) ("In thirty-eight of the states with breach notification laws, companies can avoid notification obligations if, after investigating the breach, they determine that the incident did not create a risk of harm for individuals whose personal information was exposed.").

138. *See* Jeff Kosseff, *Notified About a Data Breach? Too Late*, WALL ST. J. (Oct. 8, 2015, 7:04 PM), https://www.wsj.com/articles/notified-about-a-data-breach-too-late-1444345445.

small and midsized companies that have small information security and legal teams. The laws also impose different requirements as to the format and content of the required notifications. For instance, many states require specific details about how the breach occurred,[139] while Massachusetts prohibits breach notices from containing such details.[140] To the extent that data breach-notification laws serve a useful purpose, it is unclear whether they actually prevent data breaches from occurring in the future and are largely punitive in nature. Theoretically, data breach-notification laws serve a deterrent function. If companies will be required to notify customers and regulators after a data breach, they may have more incentive to invest in cybersecurity safeguards. However, there is little research that demonstrates a deterrent effect of data breach-notification laws. In fact, a recent RAND study found that more than 25% of U.S. adults had received a data breach notification in the previous year, and nearly 90% of them continued to conduct business with the company that sent the breach notice.[141]

Even to the extent that data breach notifications deter some future breaches, they only address a small part of the cybersecurity landscape. The breach-notification laws, like data security laws, focus entirely on confidentiality of data rather than on integrity or availability. If a cyberattack knocks Internet-connected cameras offline, for example, the camera manufacturer is not required to report the incident to consumers or regulators.

This is not to say that breach notifications are unnecessary. Notification requirements might help some customers avoid identity theft and other harms by alerting them of the possible misuse of their personal information. Moreover, the public shame of providing breach notifications might encourage some companies to invest in security safeguards.[142] However, policymakers should question whether compliance with nearly 50 separate breach notification laws is the most efficient use of a company's time in the days after a data breach. A uniform national breach-notification law might accomplish the same goals as the existing system, while allowing companies to more efficiently provide the notices and devote their limited resources to

139. *See, e.g.*, N.C. GEN. STAT. §§ 75-61, 75-65 (2016).

140. MASS. GEN. LAWS ch. 93H, §§ 1–6 (2016).

141. LILLIAN ABLON ET AL., RAND CORP., CONSUMER ATTITUDES TOWARD DATA BREACH NOTIFICATIONS AND LOSS OF PERSONAL INFORMATION 13, 27–28 (2016), https://www.rand.org/pubs/research_reports/RR1187.readonline.html ("[T]he 'sunlight' brought to the company through required notifications may not be having much effect on consumers. Indeed, information disclosure can be a useful policy device, but only to the extent that those consuming the information care about it.").

142. *See* Richard J. Sullivan & Jesse Leigh Maniff, *Data Breach Notification Laws*, 101 FED. RES. BANK KAN. CITY ECON. REV. 65, 77 (2016) ("We find states with provisions that signal active state enforcement have lower rates of identity theft. Likewise, states with provisions that provide incentives to organizations to comply with notification requirements have lower identity theft.").

other important cybersecurity tasks, such as remediating harm and preventing future incidents.

C. DATA SECURITY LITIGATION

In addition to data security and breach-notification statutes, companies face a variety of post-data breach legal claims in consumer class action lawsuits. Many of these lawsuits arise from common law claims such as negligence,[143] negligent misrepresentation,[144] breach of contract,[145] breach of implied warranty,[146] and unjust enrichment.[147] Additionally, some data breach lawsuits are brought under state consumer-protection statutes, which, like the Federal Trade Commission Act, prohibit unfair or deceptive trade practices.[148]

Perhaps the biggest barrier to these cases is a division among courts as to whether plaintiffs have Article III standing to bring the lawsuit. Some courts will only allow lawsuits to proceed if the plaintiffs have suffered actual harm, such as identity theft,[149] while others take a broader view and allow lawsuits to proceed based on the prospect of future harm.[150] Under the broader view, the mere anxiety of the possibility of identity theft is sufficient injury to provide a plaintiff with standing.[151] The lack of certainty about standing reduces the likelihood that the prospect of data security litigation will cause companies to significantly invest in cybersecurity safeguards. Data security litigation may be more forward-looking than data security and breach-notification statutes, in that it provides companies with even greater incentives to prevent future breaches. The prospect of multimillion-dollar damages or settlements could be enough to deter lax cybersecurity. Moreover, class action lawsuits often attract a great deal of publicity and typically require notice to all affected consumers, so litigation can harm a company's brand. However, like the data security statutes, data security litigation focuses only on protecting confidentiality and individual privacy, and it does little to address broader cybersecurity concerns.

There is little research that documents whether the threat of data security litigation has actually encouraged companies to adopt stronger cybersecurity protections, and companies increasingly are purchasing insurance policies

143. *See, e.g.*, *In re* Sony Gaming Networks & Customer Data Sec. Breach Litig., 996 F. Supp. 2d 942, 963 (S.D. Cal. 2014).

144. *See, e.g.*, *In re* Zappos.com, Inc., No. 3:12-cv-00325-RCJ-VPC, 2013 WL 4830497, at *3–4 (D. Nev. Sept. 9, 2013).

145. *See, e.g.*, *In re* Anthem, Inc. Data Breach Litig., 162 F. Supp. 3d 953, 970 (N.D. Cal. 2016).

146. *See, e.g.*, *In re* Hannaford Bros. Co. Customer Data Sec. Breach Litig., 613 F. Supp. 2d 108, 119–20 (D. Me. 2009), *aff'd*, Anderson v. Hannaford Bros. Co., 659 F.3d 151 (1st Cir. 2011).

147. *See, e.g.*, *In re* Target Corp. Customer Data Sec. Breach Litig., 66 F. Supp. 3d 1154, 1177–78 (D. Minn. 2014).

148. *Id.* at 1161–62.

149. *See, e.g.*, Reilly v. Ceridian Corp., 664 F.3d 38, 46 (3d Cir. 2011).

150. Krottner v. Starbucks Corp., 628 F.3d 1139, 1142–43 (9th Cir. 2010).

151. *See id.* at 1142.

that cover judgments or settlements in data security litigation. Some critics argue that cyber-insurance creates a moral hazard that reduces any incentives that a company might have to invest in cybersecurity.[152]

Even if the prospect of data security litigation is sufficient to change a company's behavior, it only affects one aspect of cybersecurity. As with data security statutes, data security litigation is primarily focused on the confidentiality of information. Lawsuits typically do not arise due to a company's failure to protect the integrity or availability of information, though it is at least possible to imagine a negligence lawsuit filed by customers who were unable to access vital medical or financial information.

D. COMPUTER HACKING LAWS

The primary computer hacking laws at the federal level are the Computer Fraud and Abuse Act ("CFAA") and the Economic Espionage Act ("EEA").[153]

The CFAA criminalizes seven different types of activities, which could generally be described as: (1) hacking to commit espionage;[154] (2) hacking to obtain information;[155] (3) hacking a federal government computer;[156] (4) hacking to commit fraud;[157] (5) hacking to commit damage;[158] (6) trafficking in passwords;[159] and (7) threats of hacking.[160] In addition to criminal penalties, the CFAA allows victims of computer hacking who have suffered damage or loss to sue under certain circumstances.[161]

Companies that have had information stolen or suffered damage to their systems or networks frequently bring civil claims under CFAA. The CFAA defines "damage" as "any impairment to the integrity or availability of data, a program, a system, or information."[162] For instance, in 2011, the United States Court of Appeals for the Sixth Circuit held that the CFAA applied to an email campaign aimed at impairing the ability of a company to send and receive

152. Liam M.D. Bailey, *Mitigating Moral Hazard in Cyber-Risk Insurance*, 3 J.L. & CYBER WARFARE 1, 5 (2014) ("Assuming that firms who seek to purchase cyber-risk insurance coverage possess a fixed budget for information security, highly priced cyber-risk insurance provides an incentive for firms to purchase indemnity from data breach costs without making a corresponding investment in the information security infrastructure necessary to protect consumer data.").

153. Each state has also passed its own computer crime statute. Some provisions are similar to those in the CFAA, while others differ. For a complete list of state computer crime statutes, see *Computer Crime Statutes*, NAT'L CONF. ST. LEGISLATURES (Dec. 5, 2016), http://www.ncsl.org/research/telecommunications-and-information-technology/computer-hacking-and-unauthorized-access-laws.aspx.

154. 18 U.S.C. § 1030(a)(1) (2012).

155. *Id.* § 1030(a)(2).

156. *Id.* § 1030(a)(3).

157. *Id.* § 1030(a)(4).

158. *Id.* § 1030(a)(5).

159. *Id.* § 1030(a)(6).

160. *Id.* § 1030(a)(7).

161. *Id.* § 1030(g).

162. *Id.* § 1030(e)(8).

emails.[163] Similarly, in 2012, a federal judge concluded that "damage" under the CFAA broadly includes "the destruction, corruption, or deletion of electronic files, the physical destruction of a hard drive, or any 'diminution in the completeness or usability of the data on a computer system.'"[164] In that respect, it is among the more comprehensive existing cybersecurity laws, as it addresses not only harms to confidentiality, but also integrity and availability. Similarly, the CFAA encompasses more areas of cybersecurity law by covering not merely harms to information, but also damage to systems or networks.

That is not to say that the CFAA is the model for cybersecurity law. For one thing, much of it was drafted more than 30 years ago, and critics argue that it has not kept up with the times.[165] Most notably, courts are deeply divided as to the scope of the CFAA. The seven provisions only apply to acts that are done "without authorization" or that "exceeds authorized access."[166] The courts are deeply divided as to whether an individual who misuses information to which she had lawful access is subject to the CFAA. The United States Court of Appeals for the Ninth Circuit has narrowly interpreted the CFAA, concluding that "[i]f Congress meant to expand the scope of criminal liability to everyone who uses a computer in violation of computer use restrictions—which may well include everyone who uses a computer—we would expect it to use language better suited to that purpose."[167] Other courts, however, have focused not only on whether the initial access was authorized, but on whether that initial access was used to further unauthorized activities.[168] The circuit court split on this issue is one example of the ambiguity of some provisions of the CFAA. Indeed, critics argue that CFAA is overly punitive, potentially exposing defendants to decades in prison.[169] For

163. Pulte Homes, Inc. v. Laborers' Int'l Union of N. Am., 648 F.3d 295, 301–02 (6th Cir. 2011) ("Because Pulte alleges that the transmissions diminished its ability to send and receive calls and e-mails, it accordingly alleges an impairment to the integrity or availability of its data and systems—i.e., statutory damage.").

164. TriTeq Lock & Sec. LLC v. Innovative Secured Sols., LLC, No. 10-cv-01304, 2012 WL 394229, at *6 (N.D. Ill. Feb. 1, 2012) (citations omitted).

165. James Hendler, *It's Time to Reform the Computer Fraud and Abuse Act*, SCI. AM. (Aug. 16, 2013), https://www.scientificamerican.com/article/its-times-reform-computer-fraud-abuse-act ("Now, in response to a reported increase in cyber attacks coming from abroad, many members of Congress want to again expand the CFAA, adding to the stringency of the law with the intent of further protecting America's computing resources.").

166. 18 U.S.C. § 1030(a)(2). The precise requirements vary by provision. For instance, section (a)(2)'s prohibition on obtaining information applies if an individual "intentionally accesses a computer without authorization or exceeds authorized access," while section (a)(5)(B)'s prohibition on recklessly causing damage to a protected computer applies only to intentional access that is done without authorization. *Id.* § 1030(a)(2), (a)(5)(B).

167. United States v. Nosal, 676 F.3d 854, 857 (9th Cir. 2012).

168. *See* United States v. Rodriguez, 628 F.3d 1258, 1263–64 (11th Cir. 2010); EF Cultural Travel BV v. Explorica, Inc., 274 F.3d 577, 582–83 (1st Cir. 2001).

169. Tim Wu, *Fixing the Worst Law in Technology*, NEW YORKER (Mar. 18, 2013), https://www.newyorker.com/news/news-desk/fixing-the-worst-law-in-technology ("Over the years, the punishments for breaking the law have grown increasingly severe—it can now put people in prison for decades for

instance, Aaron Swartz was indicted for 11 counts of CFAA violations arising from allegedly downloading millions of academic articles from a school's access to a proprietary database, exposing him to up to 35 years in prison.[170] Swartz committed suicide before going to trial, and many critics of CFAA have used his case to criticize the "disproportionate" nature of the CFAA and computer crime laws in general.[171]

The CFAA also has attracted criticism from some commentators for its likely—though far from certain—prohibition on the ability of private parties to "hack back" against those that attack them.[172] This is seen as ultimately constraining the ability of the private sector to mitigate and prevent cyberattacks, and some scholars and lawmakers have proposed amending the CFAA to explicitly allow companies to obtain information from and damage the systems of hackers.[173]

Although the CFAA is the primary on-point federal statute for computer hacking, prosecutors and private parties also use the EEA against cyber criminals. This Act prohibits individuals from stealing, copying, receiving, or possessing trade secrets without authorization if the individuals either (1) "intend[ed] or kn[ew] that the offense [would] benefit any foreign government, foreign instrumentality, or foreign agent"[174] or (2) acted for the "benefit of anyone other than the [trade secret's] owner."[175] The statute imposes criminal penalties, and it recently was amended to allow victims of trade secret misappropriation to bring civil actions.[176]

---

actions that cause no real economic or physical harm. It is, in short, a nightmare for a country that calls itself free.").

170. Superseding Indictment at 10–15, United States v. Swartz, 945 F. Supp. 2d 216 (D. Mass. 2013) (No. 1:11-cr-10260-NMG), 2012 WL 4341933.

171. Justin Peters, *Congress Has a Chance to Fix its Bad "Internet Crime" Law*, SLATE (Apr. 24, 2015, 5:47 PM), http://www.slate.com/articles/technology/technology/2015/04/aaron_s_law_why_it_s_needed_to_fix_the_horrendously_bad_cfaa.html ("[T]he laxity with which these laws have been conceived and amended—and the increasing severity of their corresponding penalties—has had serious consequences.").

172. Paul Rosenzweig, *International Law and Private Actor Active Cyber Defensive Measures*, 50 STAN. J. INT'L L. 103, 104 (2014) ("In the United States, scholars have begun to debate the legality of hack back. To date, that examination has focused exclusively on domestic U.S. law. The discussion is inconclusive, though it is probably fair to say that the weight of analysis favors the conclusion that active hack back by private sector U.S. actors violates the Computer Fraud and Abuse Act (CFAA)." (footnote omitted)); Robert Chesney, *Legislative Hackback: Notes on the Active Cyber Defense Certainty Act Discussion Draft*, LAWFARE (Mar. 7, 2017, 10:30 AM), https://www.lawfareblog.com/legislative-hackback-notes-active-cyber-defense-certainty-act-discussion-draft (describing the discussion draft of the Active Cyber Defense Certainty Act, proposed by Representative Tom Graves, which would exempt "active cyber defense measures" from liability under the CFAA).

173. Rosenzweig, *supra* note 172, at 104 ("[L]aws that are made, after all, can be unmade. And if we were to conclude as a matter of policy that it is appropriate to allow private sector actors to conduct active hack back defense, there might well be an appetite to change the law.").

174. 18 U.S.C. § 1831(a) (2012).

175. *Id.* § 1832(a).

176. *Id.* § 1836(a).

Congress passed the EEA in 1996, recognizing that the proliferation of computers "enables rapid and surreptitious duplications of the information."[177] Since its passage, the government has prosecuted a number of cases in which the defendants allegedly stole trade secrets, often from their former employers, to benefit another company or nation.[178] The recent revisions that allow civil claims arising from trade secret theft likely will increase the Act's use in cyber-theft cases.

Unlike the CFAA, which is more broadly focused on the theft of data and damage to systems and networks, the EEA focuses on the *confidentiality* of data. In that sense, the EEA addresses the same narrow avenue of cybersecurity law as many of the other protections. Although the EEA is particularly effective at addressing insider threats from employees and others who already have authorized access to trade secrets,[179] it is rare to see the Act be used to prosecute or bring claims against external hackers.

Moreover, the EEA is narrowly focused on protecting the confidentiality of certain types of information. The EEA only applies to trade secrets and therefore would not penalize the theft of personal information that does not qualify for trade secret protection. Likewise, the EEA does not impose criminal or civil penalties on hackers who launch attacks on systems or networks, or who threaten the availability or integrity of information. For instance, a ransomware campaign that shuts down a company's internal servers for a week probably would not violate the EEA, as the campaign would not involve the theft of trade secrets.

E. ELECTRONIC COMMUNICATIONS PRIVACY ACT

Restrictions on the ability of the public and private sectors to access electronic data often are associated with cybersecurity, although there is an equally strong argument that they primarily are privacy laws. The Electronic Communications Privacy Act ("ECPA") is the primary federal restriction on electronic surveillance by public and private actors. ECPA consists of three separate statutes: (1) the Wiretap Act (which restricts the surveillance of communications content while it is in transit);[180] (2) the Stored Communications Act (which restricts the surveillance of communications content while it is in storage);[181] and (3) the Pen Register Act (which restricts

177. H.R. REP. NO. 104-788, at 5 (1996) ("Hundreds of pages of information can be loaded onto a small computer diskette, placed into a coat pocket, and taken from the legal owner.").

178. *See generally, e.g.*, United States v. Hanjuan Jin, 733 F.3d 718 (7th Cir. 2013) (affirming the conviction of a naturalized American citizen of Chinese origin who stole trade secrets from her employer).

179. *See generally, e.g.*, United States v. Aleynikov, 676 F.3d 71 (2d Cir. 2012).

180. 18 U.S.C. §§ 2510–22.

181. *Id.* §§ 2701–12.

the use of devices to collect metadata, such as phone numbers dialed and email addresses in the "to" and "from" headers).[182]

The ECPA is an attempt to codify into statute some of the Fourth Amendment protections against unreasonable searches and seizures of electronic data, though it has faced some criticism for failing to adequately protect certain data—in part due to the failure of Congress to significantly update the statute since 1986.[183] However, the statutes go beyond restrictions on government surveillance. They also restrict the ability of private parties to monitor user data or share it with other parties, including the government.[184]

To be sure, the ECPA contains a number of exceptions that allow service providers to monitor networks and share information with the government.[185] However, even narrow restrictions on monitoring and disclosure may make it more difficult for the government and private sector to work together to combat cyber-threats.

That is not to say that the ECPA's restrictions on access to data are misplaced. Indeed, they are fundamental to protecting privacy and preventing government and corporate overreach. But these privacy protections do, to at least some extent, stifle the potential for cooperation between the government and the private sector in achieving better cybersecurity. As we assess how our existing laws contribute to our new conception of cybersecurity law, we must assess how they encourage or impede such collaboration.

F. THE CYBERSECURITY ACT OF 2015

The Cybersecurity Act of 2015 is an attempt to address impediments to such collaboration between the public and private sectors. Although, as discussed in the Introduction to this Article, the statute does not explicitly define "cybersecurity," it covers the field of cybersecurity law better than any

182. *Id.* §§ 3121–27.

183. United States v. Warshak, 631 F.3d 266, 288 (6th Cir. 2010) ("Moreover, to the extent that the [ECPA] purports to permit the government to obtain such emails warrantlessly, the [ECPA] is unconstitutional.").

184. *See Cybersecurity: Preventing Terrorist Attacks and Protecting Privacy in Cyberspace: Hearing Before the Subcomm. on Terrorism and Homeland Sec. of the S. Judiciary Comm.*, 111th Cong. 118 (2009) (statement of Gregory T. Nojeim), https://www.gpo.gov/fdsys/pkg/CHRG-111shrg61662/pdf/CHRG-111shrg61662.pdf ("These provisions do not, in our view, authorize ongoing or routine disclosure of traffic by the private sector to the government. To interpret them so broadly would destroy the promise of privacy in the Wiretap Act and ECPA.").

185. *See, e.g.*, 18 U.S.C. § 2702(b)(5) ("A provider described in subsection (a) may divulge the contents of a communication . . . as may be necessarily incident to the rendition of the service or to the protection of the rights or property of the provider of that service . . . ."); *id.* § 2511(2)(i) (allowing the government to intercept wire or electronic communications of a computer trespasser with consent of the computer owner, provided that the government "has reasonable grounds to believe that the contents of the computer trespasser's communications will be relevant to the investigation" and the "interception does not acquire communications other than those transmitted to or from the computer trespasser").

other single statute. In that sense, the Cybersecurity Act is the statute that is most closely focused on this Article's conception of cybersecurity law.

Among the many provisions of the Cybersecurity Act are provisions that allow private entities to: (1) monitor information systems for cybersecurity purposes;[186] (2) operate "defensive measures" for cybersecurity purposes;[187] and (3) share information about cyber-threat indicators or defensive measures with other private entities or the federal government.[188] These provisions abrogate some of the ECPA's limits on monitoring and disclosure, described above, though the extent of the abrogation is unclear because no court has yet applied the Cybersecurity Act to privacy claims.

The Cybersecurity Act provides limited protection from liability for companies that monitor information systems under the statute or share or receive cyber-threat indicators.[189] However, this open-ended communication can pose problems. Despite requirements for private entities to take steps to remove personal information before sharing cyber-threat indicators,[190] critics attacked the statute for potentially immunizing companies that violate individuals' privacy rights while not necessarily helping companies improve their cybersecurity.[191] The lengthy and spirited debate over the law demonstrates the tension that is often present between privacy protections and collaborative cybersecurity efforts.

Although the privacy concerns are well-founded, the statute—and the DHS's implementation of the sharing law—provide fairly strong safeguards to reduce the likelihood of privacy violations. It remains to be seen the extent to which the Cybersecurity Act improves cybersecurity, as agencies are still in the process of implementing it.

186. 6 U.S.C. § 1503(a)(1) (2012).

187. *Id.* § 1503(b). The statute defines "defensive measure" as "an action, device, procedure, signature, technique, or other measure applied to an information system or information that is stored on, processed by, or transiting an information system that detects, prevents, or mitigates a known or suspected cybersecurity threat or security vulnerability," and explicitly excludes any "measure that destroys, renders unusable, provides unauthorized access to, or substantially harms an information system or information stored on, processed by, or transiting such information system" and is not owned by the entity operating the defensive measure or another entity that has provided consent. *Id.* § 1501(7)(A)–(B).

188. *Id.* § 1503(c)(1).

189. *Id.* § 1505(a)–(b).

190. *Id.* § 1503(d)(1)–(2).

191. Jennifer Granick, *OmniCISA Pits DHS Against the FCC and FTC on User Privacy*, JUST SECURITY (Dec. 16, 2015, 6:09 PM), https://www.justsecurity.org/28386/omnicisa-pits-government-against-self-privacy ("Information sharing, generally a good thing, . . . nevertheless is not going to make a huge cybersecurity difference. Security experts and a bi-partisan coalition of privacy groups told Congress that we don't need to waive communications privacy laws—as OmniCISA does—to promote sharing of threat signatures. So why are we sacrificing even more American privacy on this altar? It's amazing that, given all we are learning about government surveillance, Congress will actually vote to *expand* the federal government's capacity to obtain personal data from private companies without court order.").

However, there is a reasonable likelihood that the Cybersecurity Act's broad approach to cybersecurity law will have a positive effect. Importantly—and unlike many of the other laws and regulations discussed in this Article—the Cybersecurity Act provides a *cooperative* framework for companies to work with the government. For three decades, cybersecurity law in the United States has developed under a primarily coercive regulatory structure, with companies and individuals facing the prospect of huge fines and other enforcement actions arising from their failure to adequately safeguard data. Those coercive statutes play an important role, and this Article in no way suggests that the Cybersecurity Act and similar statutes *replace* them. Rather, the Cybersecurity Act's proactive and cooperative measures compliment those of the CFAA, data security statutes, and other coercive regulations.

Additionally, the Cybersecurity Act's broad approach contemplates not only threats to confidentiality, but also to integrity and availability, as it focuses on information, systems, *and* networks. Consider, for instance, the definition of "cyber threat indicators" that companies may share:

> [I]nformation that is necessary to describe or identify—
>
> (A) malicious reconnaissance, including anomalous patterns of communications that appear to be transmitted for the purpose of gathering technical information related to a cybersecurity threat or security vulnerability;
>
> (B) a method of defeating a security control or exploitation of a security vulnerability;
>
> (C) a security vulnerability, including anomalous activity that appears to indicate the existence of a security vulnerability;
>
> (D) a method of causing a user with legitimate access to an information system or information that is stored on, processed by, or transiting an information system to unwittingly enable the defeat of a security control or exploitation of a security vulnerability;
>
> (E) malicious cyber command and control;
>
> (F) the actual or potential harm caused by an incident, including a description of the information exfiltrated as a result of a particular cybersecurity threat;
>
> (G) any other attribute of a cybersecurity threat, if disclosure of such attribute is not otherwise prohibited by law; or
>
> (H) any combination thereof.[192]

This definition contemplates not only threats to the confidentiality of data, but also access that could result in the unauthorized modification or unavailability of data, systems, and networks. More than many of the other

192. 6 U.S.C. § 1501(6).

prominent cybersecurity laws, this statute broadly addresses a range of modern cybersecurity threats.

Relatedly, while the Cybersecurity Act may encourage companies to improve their cybersecurity to prevent data breaches (and therefore promote individual privacy), the Cybersecurity Act also helps to address threats to companies' business operations (by allowing the sharing of information about DDOS attacks) and to national security (by allowing companies and the government to more agilely cooperate and identify emerging threats).

V. KEY GAPS IN CYBERSECURITY LAW

Part IV demonstrated that many current laws address the same aspects of our definition of "cybersecurity law." These laws tend to focus on confidentiality of information. The laws are punitive, primarily penalizing past bad behavior. The laws focus largely on individual rights and privacy. Finally, the laws are largely coercive regulations.

This Article does not suggest that such laws must be entirely repealed. Indeed, they play an important role in our developing cybersecurity legal framework. However, there are some areas of cybersecurity law that deserve more attention. I briefly point to four such areas where these gaps exist: (1) integrity and availability; (2) economic interests and national security; (3) cooperative laws; and (4) forward-looking laws.

A. INTEGRITY AND AVAILABILITY

As discussed above, confidentiality is an overwhelming focus of many of our cybersecurity laws. Such a focus is necessary and understandable, as confidentiality is closely linked to privacy, and privacy law has existed for more than a century, long before the development of the modern computer. Indeed, confidentiality is easily addressed in regulatory requirements that result in liability for companies that experience data breaches. However, cybersecurity laws should focus not exclusively on threats to confidentiality, but also on threats to integrity (such as the deletion of important trade secrets or website defacement) and availability (such as denial-of-service attacks).

Computer crime statutes such as the CFAA are capable of addressing some threats to integrity and availability. The CFAA could be read to criminalize and bring civil actions arising from many common attacks on integrity and availability, such as the deletion of data.[193] Unfortunately, many of these attacks come from foreign countries, such as China, Iran, North Korea, and Russia.[194] These four nations are not among the 50 nations to

193. *See, e.g.*, Int'l Airport Ctrs., L.L.C. v. Citrin, 440 F.3d 418, 419 (7th Cir. 2006) (allowing CFAA claims to proceed against the defendant who deleted data from his former employer's computer system).

194. *See Emerging Cyber Threats to the United States: Hearing Before the Subcomm. on Cybersecurity, Infrastructure Prot., and Sec. Tech.*, 114th Cong. 13–21 (2016) (written testimony of Frank J. Cilluffo, Associate Vice President and Director, Center for Cyber and Homeland Security, George

ratify the Budapest Convention on Cybercrime, which sets forth extradition procedures for cybercrime cases and minimum requirements for cybercrime laws.[195] In other words, even if the U.S. government identifies a hacker and brings charges, that individual may be out of reach of U.S. courts.

Accordingly, criminal law alone likely will not solve integrity and availability problems such as website defacement and DDOS attacks. Proactive assistance from the government—such as the National Institute of Technology and Standards' Cybersecurity Framework—can help to equip companies (and state and local governments) to better address threats to integrity and availability.

Particularly as vehicles, industrial plants, and other physical systems are increasingly connected to the Internet, the integrity and availability of systems and networks will become more crucial to private- and public-sector interests. Perhaps the federal government will need to do more than provide companies with information about ongoing threats and develop common cyber-standards. To truly ensure the availability of connected systems and networks, the government may need to entirely rethink its approach to cybersecurity assistance and take a more active role during widespread cybersecurity incidents. Just as the Federal Emergency Management Agency is the de facto coordinator of responses to natural disasters such as hurricanes and tornadoes, the federal government could consider developing a similar robust presence for cyberspace. Such government assistance would inevitably focus on integrity and availability, preventing critical private-sector services from being knocked offline or disrupted by cyberattacks.

Refocusing U.S. cybersecurity laws on integrity and availability would not be an easy task. Because many of our cybersecurity-related laws originate from the much more established conceptions of privacy, these laws have an understandable focus on the confidentiality prong of the CIA triad. To truly address the emerging cybersecurity threats that companies and the public sector confront every day, policymakers will need to place equal emphasis on integrity and availability.

B. NATIONAL SECURITY AND ECONOMIC INTERESTS

The primary goal of many existing cybersecurity laws is to protect individual privacy. To be sure, privacy always should remain an ultimate goal of cybersecurity law. However, cybersecurity law also should have the goals of helping to protect national security, as well as helping companies protect their economic interests. The Cybersecurity Act is an example of how the government can achieve these goals. The statute implicitly recognizes that companies and the federal government share an interest in securing

Washington University) (describing primary cyber-threats to United States originating from China, Iran, North Korea, and Russia).

195. Convention on Cybercrime, Nov. 23, 2001, Treaty Doc. 108–11, ETS No. 185.

information, systems, and networks, and are positioned to work toward a common goal of societal security.

When policymakers consider proposals to encourage improvements to private-sector cybersecurity, they should not only view the proposals as benefitting an individual company's bottom line, but as a vital issue for the U.S. economy. For instance, rather than merely evaluating the costs of cybersecurity tax incentives, the government should also consider the corresponding macroeconomic benefits of a cyberspace with fewer attacks and greater consumer confidence. A successful cyberattack on the electric grid, for example, could have disastrous effects not only to the targeted utility operators, but to all companies that depend on those utilities for electricity.

Similarly, the United States must view cybersecurity as a national security issue, as seen most recently in the reports of Russian interference in the 2016 U.S. elections. A focus on national security will require closer cooperation between the United States and other nations, in recognition of the truly global nature of cybersecurity threats, attacks, and challenges. The Budapest Convention is a step toward addressing cybersecurity in a more global context, though the lack of participation from China, Russia, and others limits the utility of the Convention as a true solution to many of our most pressing cybersecurity threats.[196]

Crafting cybersecurity laws with a national security and macroeconomic focus also requires a closer alignment of the government's cyber-functions. The United States does not have a Department of Cybersecurity. Instead, the responsibilities are spread throughout many agencies, some better resourced and skilled than others. Perhaps the most skilled cybersecurity professionals in the United States work at the National Security Agency, a Title 50 intelligence agency within the Department of Defense. For roughly a decade, the NSA Director also has been the head of the U.S. Cyber Command, the military's lead Title 10 (traditional military) cyber branch, though the NSA and Cyber Command are in the process of separating.[197] Cybersecurity of *civilian* government agencies is headed by a division deep within the organizational chart of the DHS, though the Office of Management and Budget is responsible for some federal agency information security policies.[198] The DHS cybersecurity division oversees the U.S. Computer Emergency Readiness Team, which exchanges cyber-threat information with the private

196. Doug Drinkwater, *Estonia President Wants China and Russia to Help Fight Cyber-Crime*, SC MEDIA UK (Jan. 26, 2015), https://www.scmagazineuk.com/estonia-president-wants-china-and-russia-to-help-fight-cyber-crime/article/537294 ("[H]e pinpointed China and Russia's failure to sign the Budapest Convention as an example that international cyber-crime collaboration remains some way off.").

197. Patrick Tucker, *What the Announced NSA/Cyber Command Split Means*, DEF. ONE (Aug. 18, 2017), http://www.defenseone.com/technology/2017/08/what-announced-nsa-cyber-command-split-means/140362.

198. *See Cyber Security Division*, DEP'T HOMELAND SECURITY, https://www.dhs.gov/science-and-technology/cyber-security-division (last visited Dec. 21, 2017).

sector.[199] During the 2016 election season, DHS offered assistance to state election officials and their private contractors, but these organizations were under no obligation to accept DHS's help.[200] And DHS plays absolutely no role in regulating private sector cybersecurity. That duty partly falls to a small office within the FTC's Bureau of Consumer Protection, at least on the federal level.[201] And the FTC is not the only federal agency to regulate cybersecurity. Other agencies across the government regulate the cybersecurity of specific industries. To name a few such examples: the Transportation Department oversees security of connected vehicles;[202] the Food and Drug Administration regulates medical device cybersecurity;[203] the Federal Energy Regulatory Commission regulates the cybersecurity of the national electric grid;[204] various financial regulatory agencies regulate financial institution cybersecurity;[205] and the Department of Health and Human Services regulates health data security.[206] Enforcement of federal cybercrime statutes such as the CFAA and EEA falls to the 94 U.S. Attorneys' Offices and the Computer Crimes and Intellectual Property Section of the U.S. Justice Department's Criminal Division.[207]

To be sure, there always will be some division of cybersecurity responsibilities among government agencies. For instance, the Posse Comitatus Act would prevent U.S. Cyber Command from enforcing civilian cybercrime laws.[208] However, the current distribution of cybersecurity responsibilities likely would benefit from some consolidation and better coordination. With so many departments of the federal government making vital decisions about cybersecurity, it is difficult to imagine how they can work

199. *Id.*

200. Alex Tin, *Ahead of Elections, States Reject Federal Help to Combat Hackers*, CBS NEWS (Oct. 28, 2016, 5:01 PM), https://www.cbsnews.com/news/ahead-of-elections-states-reject-federal-help-to-combat-hackers ("CBS News has found that 11 states—including the battlegrounds of New Hampshire and Michigan—have not accepted the Department of Homeland Security's help to try and bolster the cyberdefenses of their voter registration systems.").

201. *See Data Security*, FED. TRADE COMMISSION, https://www.ftc.gov/tips-advice/business-center/privacy-and-security/data-security (last visited Dec. 21, 2017).

202. *Vehicle Cybersecurity*, NAT'L HIGHWAY TRAFFIC SAFETY ADMIN., https://www.nhtsa.gov/technology-innovation/vehicle-cybersecurity (last visited Dec. 21, 2017).

203. *Cybersecurity*, U.S. FOOD & DRUG ADMIN., https://www.fda.gov/MedicalDevices/DigitalHealth/ucm373213.htm (last visited Dec. 21, 2017).

204. Press Release, Fed. Energy Regulatory Comm'n, FERC Directs Development of Standards for Supply Chain Cyber Controls (July 21, 2016), https://www.ferc.gov/media/news-releases/2016/2016-3/07-21-16-E-8.asp.

205. *See* 15 U.S.C. § 6801 (2012).

206. 45 C.F.R. § 164.308 (2016).

207. *See Computer Crime and Intellectual Property Section (CCIPS)*, U.S. JUST. DEP'T, https://www.justice.gov/criminal-ccips (last visited Dec. 21, 2017).

208. *See* United States v. Dreyer, 767 F.3d 826, 827 (9th Cir. 2014) (concluding that a Naval Criminal Investigative Service agent's cyber-investigation of a civilian "constituted improper military enforcement of civilian laws").

with any degree of precision to achieve common economic and national security goals. Crafting cybersecurity laws that advance macroeconomic and national security interests will require a close look at whether this web of military and civilian agencies is capable of coordinating strategies to meet these goals. At the very least, there should be better coordination among the various agencies to ensure that cybersecurity policies work toward a common goal.

C. COOPERATIVE LAWS

Relatedly, few U.S. cybersecurity laws provide companies with incentives to adopt adequate cybersecurity safeguards. While sticks often are necessary, carrots can be equally useful. The Cybersecurity Act is a step in this direction, as it creates an information-sharing platform and encourages companies to participate. Similarly, the government should consider further steps to assist companies with cybersecurity. While large companies may dedicate dozens of staffers to information security, small businesses often do not have the resources to have even a single dedicated information-security staffer. This disparity is particularly concerning because small and midsized businesses are reported to constitute the majority of all cyberattack victims.[209] Accordingly, government resources that help small businesses prepare for cyberattacks could be a worthwhile investment.

Moreover, policymakers should consider the possibility of providing economic incentives for companies to adopt cybersecurity measures. In 2013, the U.S. Treasury Department recommended against consideration of such incentives, concluding that they "would come at the expense of foregone revenue for the government or reallocation of existing fiscal obligations."[210] This conclusion is true, but not necessarily a reason to dismiss the possibility of providing well-constructed, and limited, tax incentives. Such incentives could take a variety of forms and could be conditioned on the adoption of specific cybersecurity safeguards. Although the incentives undoubtedly would reduce short-term tax revenues, the government should conduct a thorough cost–benefit analysis to understand the potential long-term benefits of such incentives. If, for instance, a tax incentive was to result in a 10% increase in cybersecurity investments and a corresponding reduction in successful cyberattacks, what would be the net impact to the U.S. economy?

209. Rosalie L. Donlon, *Small, Mid-Sized Businesses Hit By 62% of All Cyber Attacks*, PROP. CASUALTY 360 (May 27, 2015), http://www.propertycasualty360.com/2015/05/27/small-mid-sized-businesses-hit-by-62-of-all-cyber ("Francis noted that 62% of cyber-breach victims are small to mid-size businesses, which are at the greatest risk for an attack. Their level of preparation is low, and the costs of customer notification alone can be enough to do a small company irreparable financial harm.").

210. U.S. DEP'T OF TREASURY, SUMMARY REPORT TO THE PRESIDENT ON CYBERSECURITY INCENTIVES PURSUANT TO EXECUTIVE ORDER 13636, at 6 (2013), https://www.treasury.gov/press-center/Documents/Treasury%20Report%20(Summary)%20to%20the%20President%20on%20Cybersecurity%20Incentives_FINAL.pdf.

Additionally, the concurrent state and federal regulation of cybersecurity also makes it particularly challenging to implement an effective system of cooperative laws. With nearly every state imposing data breach-notification requirements, and a dozen states requiring companies to take specific steps to safeguard personal information,[211] it is difficult to align a set of effective cybersecurity incentives that apply to companies with national operations. For instance, imagine if the federal government provided companies with tax credits for adhering to a particularly stringent set of NIST-developed cybersecurity controls. Those controls may specify different standards for encryption, access control, and other requirements than the laws of some states. The inherently interstate (and global) nature of cybersecurity threats requires us to take a close look at whether it is possible—or practical—for states to continue to exercise such control over the future of U.S. cybersecurity law.

Even within the federal government, the scattered cybersecurity responsibilities make it difficult to establish an effective system of both coercive and cooperative cybersecurity laws, just as the current federal structure impedes work toward economic and national security interests. Regulatory agencies such as the FTC and the Department of Health and Human Services penalize companies for inadequate data security. These agencies are charged with the coercive cybersecurity laws. DHS and NIST provide cooperative assistance, sharing cyber-threat information and suggesting best practices for cybersecurity. The FTC, for example, is under no obligation to align its penalties for inadequate cybersecurity with the best practices suggested by NIST. Nor must NIST suggest cybersecurity standards that satisfy the FTC's regulatory expectations.[212]

Imagine, for instance, a two-tiered data security law. The first tier contains bare-minimum data security requirements, such as mandatory password changes every 90 days, encryption of health and financial data, and the use of standard firewall and antivirus programs on systems that store personal information. A company that fails to satisfy this first tier of data security standards could face regulatory fines or private lawsuits if customers experience a data breach. That would be the coercive portion of the data security law. But the law would contain a second tier, with optional data security standards that are far more rigorous than those in the first tier. These standards might include annual cybersecurity audits, encryption of all personal information while in transit and storage, mandatory assessments of the cybersecurity practices of third-party service providers, restrictions on the ability of employees to access sensitive data remotely, and strict limits on physical access to rooms that contain media that store personal

211. *See supra* Parts IV.A–B.

212. *See supra* Part IV.A.

information.[213] If an independent auditor annually verifies that a company meets these stringent criteria, the company would receive certain benefits, such as a tax credit, limited immunity from data security-related litigation, or merely a designation of cyber-readiness from the government, making it more attractive to potential customers.

D. FORWARD-LOOKING LAWS

Many U.S. cybersecurity laws, including data security statutes and breach-notification laws, are largely backward-looking. Of course, data security laws require companies to adopt certain requirements, but companies typically face lawsuits or enforcement actions under those statutes *after* a data breach has occurred. By shifting toward a more cooperative framework for cybersecurity laws, the United States also would take a more forward-looking approach and help companies prevent data breaches and other cybersecurity attacks from ever occurring in the first place.

Data breach-notification laws are perhaps the greatest demonstration that the current cybersecurity legal framework is backward-looking, not forward-looking. When a data breach occurs, companies must examine the laws of 48 states and the District of Columbia, as well as federal laws if they handle sensitive data such as health or financial information. Companies must review details of the breach to determine if the compromised information falls into each statute's definition of "personal information" and whether an exception to each of the laws applies. If any of the laws require notice, the companies then must carefully draft a notice to each consumer to ensure that they meet each state's procedural requirements. In the meantime, the companies are not devoting these resources to fixing the vulnerability that caused the breach in the first place, or preventing future attacks.

A move toward forward-looking laws is consistent with an emphasis on a cybersecurity legal framework that emphasizes cooperation between the government and the private sector. It is easier to conceive of the government and private sector working together to prevent future attacks than it is to envision them cooperating on determining punishment for past cybersecurity incidents.

VI. CONCLUSION

This Article has attempted to formulate a definition of "cybersecurity law" that broadly encompasses our modern conception of cybersecurity, and addresses the most significant cyber-threats that the United States currently confronts. Of course, this definition is only one formulation, based on our nation's current cybersecurity threats. This Article does not advocate for specific policy changes to improve cybersecurity. Rather, it identifies the key

213. *See, e.g.*, U.S. DEP'T OF COMMERCE, *supra* note 87, at 10–14 (providing a list of safeguards for federal government contractors that handle sensitive unclassified information).

areas of cybersecurity law that are not addressed adequately by current U.S. laws. As policymakers and courts continue to address cybersecurity law, it is increasingly important that they use a common taxonomy and have an understanding of all areas that should be covered by their statutes, regulations, and court rulings.

Providing a taxonomy and a proposed set of goals is only the first step toward focusing the U.S. legal system on the actual cyber-threats that the public and private sector face. This common definition and aspiration will allow for coherence and a broad framework as scholars, policymakers, and legislators evaluate our existing laws and consider new policies. Part V of this Article provides a starting point for discussion as to how U.S. laws could better achieve the ultimate goals of cybersecurity. Future scholarship can use this definition and these goals to propose solutions to evolving cybersecurity threats.