Tennessee Law Review

Volume 88
Issue 1 *Fall 2020*

Article 4

2020

AVAILABILITY'S LAW

Ido Kilovaty

AVAILABILITY'S LAW

IDO KILOVATY*

---

* Frederic Dorwart and Zedalis Family Fund Endowed Assistant Professor of Law, University of Tulsa, College of Law; Cybersecurity Policy Fellow, New America; Visiting Faculty Fellow, Center for Global Legal Challenges, Yale Law School; Affiliated Fellow, Information Society Project, Yale Law School. The author wishes to thank the terrific student editors at the *Tennessee Law Review* who edited this Article, including Doug Campbell, Braxton Kinney, Jesse Small, Morgan Webber, Johnny Cerisano, Joshua Ferrell, Becca Plank, and Kaleb Byars.

Cybersecurity incidents affecting the availability of computers, networks, and data are on the rise. Distributed denial-of-service and ransomware attacks can bring down critical systems and databases, making them unavailable when most needed, potentially affecting every individual, industry, sector, and branch of government. This Article critically evaluates cybersecurity law's gap in addressing the growing threat of availability attacks to information technology systems. While cybersecurity law is defined as the legal framework that "promotes the confidentiality, integrity, and availability of public and private information, systems, and networks . . . .", this Article argues that cybersecurity law is overwhelmingly concerned with confidentiality and integrity, often to the exclusion of availability. This Article offers a theory as to why availability is so often ignored by cybersecurity law, and why it should not be. This Article also acknowledges that while cybersecurity law at present is unsatisfactory, certain regulatory and market-based solutions can alleviate the risks arising from availability threats that are currently not covered by the law.

INTRODUCTION

On October 21, 2016, the Domain Name System[1] provider Dyn experienced a massive distributed denial-of-service (DDoS) attack targeting its servers.[2] While the DDoS attack on Dyn would certainly be characterized as a cybersecurity incident, it was not a "data breach."[3] The attackers did not seem to be interested in any consumers' personal information that the Dyn servers may have contained.[4] As with other DDoS attacks, the purpose of the attack was

---

1. Chris Gonyea, *DNS: Why It's Important and How It Works*, DYN (Aug. 9, 2018), https://dyn.com/blog/dns-why-its-important-how-it-works [https://web.archive.org/web/20180810235801/https://dyn.com/blog/dns-why-its-important-how-it-works/] ("The Domain Name System (DNS) is a distributed directory that resolves human-readable hostnames, such as www.dyn.com, into machine-readable IP addresses like 50.16.85.103.").

2. Brian Krebs, *DDoS on Dyn Impacts Twitter, Spotify, Reddit*, KREBS ON SEC. (Oct. 21, 2016), https://krebsonsecurity.com/2016/10/ddos-on-dyn-impacts-twitter-spotify-reddit.

3. Nicole Martin, *What Is a Data Breach?*, FORBES (Feb. 25, 2019), https://www.forbes.com/sites/nicolemartin1/2019/02/25/what-is-a-data-breach/#3b1e682a14bb ("A data breach . . . allows hackers to access customer data [to use] this information for identity theft and fraud purposes.").

4. Bruce Schneier, *Lessons from the Dyn DDoS Attack*, SCHNEIER ON SEC. (Nov. 8, 2016, 6:25 AM), https://www.schneier.com/blog/archives/2016/11/lessons_

to overwhelm Dyn's servers with an enormous volume of bogus requests so that legitimate end-users could not access Dyn's lookup services, which translate web addresses to numerical IP addresses, establishing a direct connection to the requested website.[5] The result was utter chaos as access to major parts of the internet, including Amazon, Spotify, and Twitter, were unavailable to users during the DDoS attack.[6]

Or consider how on January 10, 2018, an Indiana hospital became the victim of a ransomware attack.[7] "Ransomware" is a malicious software that encrypts valuable data, such as medical data, barring access to it until a ransom is paid to the attackers.[8] Hospitals,[9] schools,[10] newspapers,[11] cities,[12] and even law enforcement agencies[13] have become valuable targets for hackers looking for quick monetary gain, usually in the form of untraceable cryptocurrency payouts by the

---

from_th_5.html ("[DDoS] attacks started out as a way to show off, then quickly transitioned to a method of intimidation, or a way of just getting back at someone you don't like.").

5. *Id.*

6. Kif Leswing, *A Massive Cyberattack Knocked out Major Websites Across the Internet*, BUS. INSIDER (Oct. 21, 2016, 9:03 PM), https://www.businessinsider.sg/amazon-spotify-twitter-github-and-etsy-down-in-apparent-dns-attack-2016-10.

7. Patrick Howell O'Neill, *Indiana Hospital Shuts Down Systems After Ransomware Attack*, CYBER SCOOP (Jan. 15, 2018), https://www.cyberscoop.com/hancock-hospital-ransomware.

8. *Ransomware*, CYBERSECURITY & INFRASTRUCTURE SEC. AGENCY, https://www.us-cert.gov/Ransomware (last visited Oct. 23, 2020) ("Ransomware is a type of malicious software, or malware, designed to deny access to a computer system or data until a ransom is paid. Ransomware typically spreads through phishing emails or by unknowingly visiting an infected website.").

9. Kim Zetter, *Why Hospitals Are the Perfect Targets for Ransomware*, WIRED (Mar. 30, 2016, 1:31 PM), https://www.wired.com/2016/03/ransomware-why-hospitals-are-the-perfect-targets.

10. Nicholas Bogel-Burroughs, *Hackers' Latest Target: School Districts*, N.Y. TIMES (July 28, 2019), https://www.nytimes.com/2019/07/28/us/hacker-school-cybersecurity.html.

11. *See, e.g.*, Malena Carollo, *Tampa Bay Times Hit by Ransomware Attack*, TAMPA BAY TIMES, https://www.tampabay.com/news/business/2020/01/23/tampa-bay-times-hit-by-ransomware-attack (last updated Jan. 24, 2020) (noting that a number of newspapers have been subject to DDoS attacks, including the *Tampa Bay Times*, *South Florida Sun-Sentinal*, and the *Chicago Tribune*).

12. *See, e.g.*, Lily Hay Newman, *Atlanta Spent $2.6M to Recover from a $52,000 Ransomware Scare*, WIRED (Apr. 23, 2018, 8:55 PM), https://www.wired.com/story/atlanta-spent-26m-recover-from-ransomware-scare (Atlanta systems attacked with ransomware).

13. Chris Francescani, *Ransomware Hackers Blackmail U.S. Police Departments*, NBC NEWS (Apr. 26, 2016), https://www.nbcnews.com/news/us-news/ransomware-hackers-blackmail-u-s-police-departments-n561746.

victims.[14] Indeed, contrary to the FBI recommendation of not paying ransom,[15] the Indiana hospital ended up paying approximately $45,000 in bitcoin in exchange for the locked data.[16] Many victims who are somehow fortunate to forgo paying the hackers still spend large amounts of money and time to recover and improve the security of their systems.[17]

The common thread to both aforementioned incidents is that they have affected the *availability* of computers, networks, and data.[18] As opposed to data *theft*, these incidents target users' ability to *access* their computers, networks, and data.[19] Availability is one of the three primary aspects on which information security focuses: confidentiality, integrity, and availability.[20] These three aspects of information security have become known as the "CIA triad"[21] and represent the very foundation of information security.[22] While the confidentiality and integrity of personal information receive the utmost attention in current cybersecurity law, availability often remains excluded or ignored.[23] The importance of the availability of

---

14. Michael Baker, *How Cryptocurrencies Are Fueling Ransomware Attacks and Other Cybercrime*, FORBES (Aug. 3, 2017, 8:00 AM), https://www.forbes.com/sites/forbestechcouncil/2017/08/03/how-cryptocurrencies-are-fueling-ransomware-attacks-and-other-cybercrimes.

15. *Ransomware Victims Urged to Report Infections to Federal Law Enforcement*, FED. BUREAU INVESTIGATION (Sept. 15, 2016), https://www.ic3.gov/media/2016/160915.aspx ("The FBI does not support paying a ransom to the adversary. Paying a ransom does not guarantee the victim will regain access to their data; in fact, some individuals or organizations are never provided with decryption keys after paying a ransom.").

16. O'Neill, *supra* note 7.

17. *See, e.g.*, Henry L. Davis, *$10 Million Cyber Attack Hits New York Hospital*, MAUREEN DATA SYS. (Feb. 13, 2018), https://www.mdsny.com/ten-million-cyber-attack-hits-new-york-hospital (noting that a ransomware attack on a New York hospital was estimated to cause $10 million in increased security expenses).

18. *Ransomware Victims Urged to Report Infections to Federal Law Enforcement*, *supra* note 15 ("Ransomware is a type of malware installed on a computer or server that encrypts the files, making them inaccessible until a specified ransom is paid.").

19. *Ransomware*, *supra* note 8.

20. *See* Andrea M. Matwyshyn, *Cyber!*, 2017 BYU L. REV. 1109, 1138 ("Security, in the technical community, historically refers to questions of data confidentiality, integrity, and availability as engineering properties of a system—questions likely to be disconnected from the identity of any individual human person.").

21. Jeff Kosseff, *Defining Cybersecurity Law*, 103 IOWA L. REV. 985, 997 (2018).

22. Debbie Walkowski, *What Is the CIA Triad?*, F5 LABS (July 9, 2019), https://www.f5.com/labs/articles/education/what-is-the-cia-triad.

23. Kosseff, *supra* note 21, at 1024 ("[C]onfidentiality is an overwhelming focus of many of our cybersecurity laws. . . . [C]ybersecurity laws should focus not exclusively on threats to confidentiality, but also on threats to integrity (such as the deletion of

computers, networks, and data is on the rise, and cybersecurity law ought to catch up.

Can the law pertaining to information security—namely cybersecurity law—respond to the aforementioned threats to availability of information technology systems the same way that it already applies to confidentiality and integrity threats? The CIA triad suggests that if we had to provide a plausible definition of cybersecurity *law*, we would likely categorize it as the "legal framework that '*promotes the confidentiality, integrity, and availability of public and private information, systems, and networks* . . . .'"[24] The interest in safeguarding availability, therefore, is equal to the interests in preserving confidentiality and integrity in the information technology context because all three aspects are equal parts of information security.

However, while the many federal and state statutes, regulations, and enforcement actions together constitute the field of cybersecurity law, this legal landscape is inadequate in that it predominately focuses on confidentiality threats to sensitive personal data.[25] As a result, availability threats remain largely unaddressed in today's cybersecurity law, leading to a considerable gap that creates underenforcement and ambiguity, and exposes consumers to serious harm.[26]

This Article explores and seeks to provide a detailed account of this gap. Primarily, this Article argues that cybersecurity law does not currently have a robust conception of the cybersecurity threats to availability. This creates a grey area in cybersecurity law, where devastating cybersecurity incidents—such as DDoS and ransomware attacks—that target the availability of computers, networks, data, and systems are not sufficiently covered by the law, and the law offers no remedy and little to no guidance to potential victims and affected third parties. In turn, this leads to ambiguity, impunity, and frustration in affected sectors and harm to consumers.[27] In addition,

---

important trade secrets or website defacement) and availability (such as denial-of-service attacks).").

24. *Id.* at 988 (emphasis added).

25. *Id.* at 998 ("U.S. cybersecurity-related laws heavily focus on only one prong of the CIA Triad: confidentiality.").

26. *See, e.g., id.* at 999 ("[E]veryday devices, ranging from medical devices to kitchen appliances to automobiles, are connected to the Internet. Imagine the chaos if hackers manage to disable thousands of pacemakers, or cause vehicles to accelerate to 100 miles per hours [sic] 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.").

27. *See id.*

to make the case for availability's law, this Article frames availability as a *human safety*, *national security*, and *infrastructure stability* issue. This Article proposes changes to cybersecurity law that better capture the need to safeguard availability—*availability's law*—and explores what such law should look like.

While the Dyn DDoS attack and the Indiana hospital ransomware provide two straightforward examples of availability attacks,[28] the threat is actually far wider and more menacing. Vehicles,[29] industrial plants,[30] the power grid,[31] and even implantable cardiac devices[32] and insulin pumps[33] all rely upon the availability of data and internet access. Other physical systems are increasingly becoming connected to the internet by default,[34] meaning that any compromise to the

---

28. I will use the term "availability attacks" to denote incidents that solely affect the availability of data and systems. While a broader definition of cyberattack is "the use of deliberate actions—perhaps over an extended period of time—to alter, disrupt, deceive, degrade, or destroy adversary computer systems or networks or the information and/or programs resident in or transiting these systems or networks," availability attacks are concerned primarily with disruptions of computer systems, networks, and data. *See* NAT'L RSCH. COUNCIL OF THE NAT'L ACADS., TECHNOLOGY, POLICY, LAW, AND ETHICS REGARDING U.S. ACQUISITION AND USE OF CYBERATTACK CAPABILITIES 80 (William A. Owens et al. eds., 2009).

29. Security researchers have recently demonstrated how vehicles can be hacked. *See* Andy Greenberg, *Hackers Remotely Kill a Jeep on the Highway—With Me in It*, WIRED (July 21, 2015, 6:00 AM), https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway.

30. *See, e.g.*, Charlie Osborne, *Hackers Use Triton Malware to Shut Down Plant, Industrial Systems*, ZDNET (Dec. 15, 2017, 9:54 AM), https://www.zdnet.com/article/hackers-use-triton-malware-to-shut-down-plant-industrial-systems.

31. Availability attacks on the electric grid may have catastrophic consequences. Evidence indicates that foreign governments may be probing the U.S. power grid. *See* Lily Hay Newman, *Russian Hackers Haven't Stopped Probing the US Power Grid*, WIRED (Nov. 28, 2018, 2:10 PM), https://www.wired.com/story/russian-hackers-us-power-grid-attacks.

32. *See, e.g.*, *Cybersecurity Vulnerabilities Affecting Medtronic Implantable Cardiac Devices, Programmers, and Home Monitors: FDA Safety Communication*, U.S. FOOD & DRUG ADMIN. (Mar. 21, 2019), https://www.fda.gov/medical-devices/safety-communications/cybersecurity-vulnerabilities-affecting-medtronic-implantable-cardiac-devices-programmers-and-home (alerting the public about "cybersecurity vulnerabilities identified in a wireless telemetry technology used for communication between Medtronic's implantable cardiac devices, clinic programmers, and home monitors").

33. *See, e.g.*, Morgan Krakow, *Insulin Pumps Are Vulnerable to Hacking, FDA Warns Amid Recall*, WASHINGTON POST (June 28, 2019, 2:35 PM), https://www.washingtonpost.com/health/2019/06/28/insulin-pumps-are-vulnerable-hacking-fda-warns-amid-recall.

34. *See* Bruce Schneier, *The Internet of Things Will Be the World's Biggest Robot*, SCHNEIER ON SEC. (Feb. 4, 2016, 6:18 AM), https://www.schneier.com/blog/archives/2016/02/the_internet_of_1.html ("Soon everything will be on the

availability of these systems and networks will become far more consequential, potentially with significant physical consequences.[35] In other words, cybersecurity is becoming synonymous with physical security.[36]

This Article has four primary objectives. The first is to introduce and explore the assertion that cybersecurity law *currently* promotes all three aspects of information security: confidentiality, integrity, and availability. This Article will argue that data security statutes, state data breach notification statutes, Federal Trade Commission (FTC) enforcement activity, and anti-hacking laws are almost exclusively focused on threats to confidentiality.

This Article's second objective is to illustrate that cybersecurity law is currently incapable of addressing specific cybersecurity incidents affecting availability that have already occurred. With the proliferation of internet-connected devices in our daily lives, availability compromises may become far more devastating. The law is not ready for this reality.

The third objective is to frame availability as forming issues of *human safety*, *national security*, and *infrastructure stability*—that is, to make the case that availability is not only about whether computers, networks, and data are available but rather a broader question of whether humans, the nation, and infrastructure are safe.

The fourth objective of this Article is to contribute to legal scholarship and the development of cybersecurity law by exploring the ways in which availability could be embedded within existing legal frameworks. This Article proposes certain regulatory and market-based solutions that could be leveraged to fill cybersecurity law's gap with regard to availability. For example, the treatment of availability threats in the Computer Fraud and Abuse Act (CFAA) may serve as a model for state computer crime statutes, and existing market-based methods and tools that seek to defend against availability attacks can

---

[i]nternet: the things we own, the things we interact with in public, autonomous things that interact with each other.").

35. Bruce Schneier, *Security and the Internet of Things*, SCHNEIER ON SEC. (Feb. 1, 2017, 8:05 AM), https://www.schneier.com/blog/archives/2017/02/security_and_th.html ("Today, the integrity and availability threats are much worse than the confidentiality threats. Once computers start affecting the world in a direct and physical manner, there are real risks to life and property. There is a fundamental difference between crashing your computer and losing your spreadsheet data[] and crashing your pacemaker and losing your life.").

36. *See, e.g.*, *id.*

infuse the general standard of *reasonable cybersecurity* with practical and actionable meaning.[37]

This Article proceeds in five parts. Part I introduces the mismatch between information security as a technical field and cybersecurity as a legal and policy matter, in particular as they pertain to availability as a cybersecurity concern. Part II looks at current cybersecurity law and how the majority of it ignores availability attacks. Part III frames the problem with the current cybersecurity law as a matter of *human safety*, *national security*, and *infrastructure stability*. In Part IV, this Article will propose a cybersecurity law for availability attacks—*availability's law*—and amendments to existing cybersecurity law that would alleviate some of the concerns surrounding availability threats. Finally, Part V concludes.

I. INFORMATION SECURITY V. CYBERSECURITY LAW

To understand why cybersecurity law fails at addressing availability threats, it is worth summarizing the difference between *information security* as a technological profession and *cybersecurity law* as a law and policy matter. This Part provides a better understanding of the gap between information security as a technical and scientific matter and cybersecurity law. It begins by introducing the basic contours of both information security and cybersecurity law. It then proceeds to identify the discrepancy between the goals of information security and the goals of cybersecurity law. While information security is a profession that has existed more or less ever since computers and data began to permeate our daily lives,[38] cybersecurity law has been on a slower and less comprehensive trajectory.[39] It concludes that this gap may leave potential victims in

---

37. *See* William McGeveran, *The Duty of Data Security*, 103 MINN. L. REV. 1135, 1176 (2019) ("FTC complaints define that duty in the negative, by condemning companies for information-handling practices that 'failed to provide *reasonable security* to prevent unauthorized access to personal information on their network.'" (emphasis added)).

38. At the very least, information security has become a matter of concern ever since the first known internet-originating malware that infected thousands of computers worldwide: the Morris Worm. *See The Morris Worm: 30 Years Since First Major Attack on the Internet*, FED. BUREAU INVESTIGATION (Nov. 2, 2018), https://www.fbi.gov/news/stories/morris-worm-30-years-since-first-major-attack-on-internet-110218.

39. *See* Matwyshyn, *supra* note 20, at 1126–27 (identifying two main legal approaches to cybersecurity—deterrence and information sharing—and arguing that these two approaches are outdated and inefficient in today's shared vulnerability landscape).

great uncertainty and expose them to unabated and devastating integrity and availability attacks.

A. What Is Information Security?

Information security seeks to protect a wide variety of valuable "assets" pertaining to computer systems.[40] These assets can take the form of "hardware, software, data, people, processes, or combinations of these."[41] As noted earlier in this Article, in order to do so, information security focuses on three distinct properties: confidentiality, integrity, and availability.[42] This "CIA triad"[43] is seen purely as "engineering properties of a system."[44]

Confidentiality seeks to ensure that assets are only viewed by authorized parties.[45] For example, a student's grades may only be viewed by the student and other predetermined authorized users.[46] A breach to confidentiality occurs when a third party, say the student's friends, gains unauthorized access to the system that stores the grades.[47]

Integrity refers to the "ability of a system to ensure that an asset is modified only by authorized parties."[48] For instance, using the previous example, only an authorized educator should be able to modify a student's grade, if such modification is warranted. A breach of integrity occurs when a third party, say the same friends of that student, decide to add (or subtract) points from their grades in an unauthorized manner.[49]

---

40. CHARLES PFLEEGER ET AL., SECURITY IN COMPUTING 2 (5th ed. 2015).

41. *Id.*

42. *See* Walkowski, *supra* note 22.

43. Ashish Agarwal & Aparna Agarwal, *The Security Risks Associated with Cloud Computing*, 1 INT'L J. COMPUT. APPLICATIONS ENG'G SCIS. (SPECIAL ISSUE) 257, 257–58 (2011).

44. *See* Matwyshyn, *supra* note 20, at 1138.

45. PFLEEGER ET AL., *supra* note 40, at 6.

46. *See, e.g.*, PFLEEGER ET AL., *supra* note 40, at 8 ("A proud student may run out of a classroom screaming 'I got an A!' but the student should be the one to choose whether to reveal that grade to others.").

47. In U.S. computer crime law, the main statute that seeks to protect information technology systems from confidentiality attacks is 18 U.S.C. § 1030(a)(2)(C) (2018), which punishes whoever "intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains . . . information from any protected computer."

48. PFLEEGER ET AL., *supra* note 40, at 6.

49. *See, e.g.*, United States v. Barrington, 648 F.3d 1178, 1191 n.11 (11th Cir. 2011) (upholding the defendant's conviction under the Wire Fraud Statute, reasoning that by changing his own and his friends' grades, the defendant committed a federal

And finally, availability pertains to the system's ability to ensure uninterrupted access to assets by authorized users.[50] For example, a student who may want to view her grade should be able to do so by accessing the grading system. An availability incident occurs when the notorious friends of that student decide once again to mess with the system, flooding it with bogus traffic that overwhelms the system which can only handle a limited amount of traffic at single point in time.

The CIA triad illustrates that information security, in the words of Jennifer Chandler, is "not a single problem, but rather a group of very different problems involving various sets of threats, targets[,] and costs."[51] While we would expect the law to address all these very different problems, in reality, it ignores a significant portion of threats to information security.

B. What Is Cybersecurity Law?

While information security and cybersecurity are generally synonymous, the latter is used more often in legal and policy circles.[52] In recent years, scholars, policymakers, and practitioners have begun to refer to the law and policy of information security as "cybersecurity law."[53] The Congressional Research Service has identified as many as fifty statutes that could be considered part of "cybersecurity law."[54] However, cybersecurity law may lend itself to multiple definitions,[55] and there is not a single authoritative definition of the term.[56] This

---

crime and that "the University certainly has an intangible property interest in the integrity of its grading system").

50. PFLEEGER ET AL., *supra* note 40, at 6.

51. Jennifer A. Chandler, *Security in Cyberspace: Combatting Distributed Denial of Service Attacks*, 1 U. OTTAWA L. & TECH. J. 231, 233 (2004).

52. *See* Matwyshyn, *supra* note 20, at 1158 ("In essence, the term 'cybersecurity' is the consequence of a cultural divide between the two coasts: 'cybersecurity' is the Washington, D.C. legal rebranding for what Silicon Valley veterans have historically usually called 'infosec' or simply 'security.'").

53. *See, e.g.*, Kosseff, *supra* note 21, at 987 (discussing lawmakers' use of the term "cybersecurity law").

54. ERIC FISCHER, CONG. RSCH. SERV., R42114, FEDERAL LAWS RELATING TO CYBERSECURITY: OVERVIEW OF MAJOR ISSUES, CURRENT LAWS, AND PROPOSED LEGISLATION 28 (2014).

55. *See, e.g.*, Orin Kerr, *What Is 'Cybersecurity Law'?*, WASHINGTON POST: VOLOKH CONSPIRACY (May 14, 2015), https://www.washingtonpost.com/news/volokh-conspiracy/wp/2015/05/14/what-is-cybersecurity-law ("If you look closely, though, there isn't much clarity about what 'cybersecurity law' actually means.").

56. *See* FISCHER, *supra* note 54, at 1 n.1 ("Thus cybersecurity, a broad and arguably somewhat fuzzy concept for which there is no consensus definition, might

Article takes the view that it is generally comprised of a patchwork of statutes and regulations that promote, or ought to promote, "*the confidentiality, integrity, and availability of public and private information, systems, and networks.*"[57]

While this definition may seem desirable and complete, the United States currently has no comprehensive statutory or regulatory framework that fits the definition of what cybersecurity law naturally ought to be.[58] Even the latest legislation on the matter, the Cybersecurity Act of 2015, does not define "cybersecurity."[59] To respond to the ambiguity of the term "cybersecurity law," Orin Kerr has suggested it is comprised of four discrete categories:[60] the law addressing the steps that victims of computer intrusions can take; the law governing the liability for computer intrusions, both for the victim and the perpetrator; the regulatory law of computer security; and special legal issues arising from government offense and defense.[61] These categories are all equally vague with respect to availability attacks.

Regardless of the preferred definition of cybersecurity law, the current legal landscape illustrates that cybersecurity law is disproportionately concerned with preserving data confidentiality, for example, through the focus on data breaches, based on a dated notion of privacy rather than security and safety.[62] As Jeff Kosseff notes, "[C]ybersecurity has taken a backseat to privacy in our current national debate, in part because policymakers often conflate the issues and claim to be addressing both."[63] Thus, it is unsurprising that

---

best be described as measures intended to protect information systems—including technology (such as devices, networks, and software), information, and associated personnel—from diverse forms of attack." (emphasis omitted)).

57. *See* Kosseff, *supra* note 21, at 988–89 (providing a definition that goes further: "[T]hrough the use of forward-looking regulations and incentives, with the goal of protecting individual rights and privacy, economic interests, and national security.").

58. Jeff Kosseff, *Hamiltonian Cybersecurity*, 54 WAKE FOREST L. REV. 155, 157 (2019).

59. *See* Kosseff, *supra* note 21, at 986.

60. Kerr, *supra* note 55.

61. *Id.*

62. This confusion is often referred to as "privacy conflation." *See* Matwyshyn, *supra* note 20, at 1135 (discussing the "analytical error" of attempting to "cram" cybersecurity law into the legal framework of privacy).

63. Jeff Kosseff, *Congress Is Finally Tackling Privacy! Now Let's Do Cybersecurity*, SLATE (Dec. 3, 2019, 3:00 PM), https://slate.com/technology/2019/12/congress-national-privacy-law-cybersecurity.html ("Privacy provides users with control over how businesses collect, use, and share their information. Cybersecurity

current cybersecurity law is disproportionately focused on confidentiality concerns.[64] This mismatch has significant consequences of which legislators must be cognizant.

C. Consequences of the Mismatch

The mismatch between the science of information security and cybersecurity law and policy may have serious consequences. First, consumers are not sufficiently protected from the consequences of availability attacks.[65] The effects of such attacks can be devastating—critical infrastructure could be disabled,[66] emergency services could become unavailable for an extended period of time,[67] and financial activity could grind to a halt.[68] Likewise, companies do not have sufficient statutory guidance on how availability attacks are defined, or what sorts of mechanisms should they employ to comply with reasonable information security requirements in this context.[69] Nor do they have sufficient incentives to defend against availability

---

prevents unauthorized parties from accessing, altering, or rendering unavailable their data, information systems, or connected devices.").

64. *See id.* ("[T]hese bills . . . typically focus on imposing vague and broad requirements to secure personal information and don't meaningfully address other vital cybersecurity concerns . . . .").

65. *See, e.g.*, Kosseff, *supra* note 21, at 999.

66. *See, e.g.*, Eduard Kovacs, *DDoS Attacks More Likely to Hit Critical Infrastructure than APTs: Europol*, SEC. WEEK (Sept. 27, 2017), https://www.securityweek.com/ddos-attacks-more-likely-hit-critical-infrastructure-apts-europol (discussing ransomware attacks that have "caused serious disruptions in sectors such as healthcare, law enforcement[,] and transportation").

67. *See, e.g.*, Jon Fingas, *Arizona Man Gets 20 Months in Prison for Emergency System DDoS Attacks*, ENGADGET (June 19, 2018), https://www.engadget.com/2018/06/19/arizona-man-sentenced-for-emergency-system-ddos (describing a ransomware attack in which a hacker targeted Madison, Wisconsin and "not only took down the city's website, but 'crippled' its emergency communication system to the point where first responders had trouble reaching the 911 center").

68. *New Zealand Stock Exchange Halted by Cyber-Attack*, BBC NEWS (Aug. 26, 2020), https://www.bbc.com/news/53918580; *see also* John McCrank, *Cyber Attacks on Stock Exchanges Put Markets at Risk: Report*, REUTERS (July 16, 2013, 6:00 PM), https://www.reuters.com/article/net-us-cybercrime-exchanges-report/cyber-attacks-on-stock-exchanges-put-markets-at-risk-report-idUSBRE96F19A20130716 (suggesting that cyberattacks could have "systemic impacts" on financial infrastructure).

69. *See* Timothy E. Deal, *Moving Beyond "Reasonable": Clarifying the FTC's Use of Its Unfairness Authority in Data Security Enforcement Actions*, 84 FORDHAM L. REV. 2227, 2243 (2016) (arguing that the FTC had not provided companies with satisfactory guidance on the meaning of "reasonable" data security).

attacks if regulation does not directly ask them to do so.[70] While reputation may be an incentive for self-regulation,[71] consumers may not even be aware that a company has experienced an availability attack as data breach notification laws do not apply to data breaches where consumer information has not been compromised.[72]

Second, not only are consumers insufficiently protected from the consequences of availability attacks, but they also may lack a remedy for the damages suffered as a result.[73] At the very outset, consumers who decide to take the matter to court may experience an Article III standing hurdle.[74] Article III of the U.S. Constitution directs the judicial branch to adjudicate "cases and controversies."[75] The

---

70. Bruce Schneier, *We Need to Save the Internet from the Internet of Things*, VICE: MOTHERBOARD (Oct. 6, 2016, 3:30 PM), https://www.vice.com/en_us/article/ezpq3m/we-need-to-save-the-internet-from-the-internet-of-things ("The market can't fix this [DDoS] because neither the buyer nor the seller cares. Think of all the CCTV cameras and DVRs used in the attack against Brian Krebs. The owners of those devices don't care. Their devices were cheap to buy, they still work, and they don't even know Brian. The sellers of those devices don't care: they're now selling newer and better models, and the original buyers only cared about price and features.").

71. Doug Drinkwater, *Does a Data Breach Really Affect Your Firm's Reputation?*, CSO ONLINE (Jan. 7, 2016, 3:55 AM), https://www.csoonline.com/article/3019283/does-a-data-breach-really-affect-your-firm-s-reputation.html.

72. *See, e.g.*, Dalmacio V. Posadas, *After the Gold Rush: The Boom of the Internet of Things, and the Busts of Data-Security and Privacy*, 28 FORDHAM INTELL. PROP. MEDIA & ENT. L.J. 69, 90 (2017) (arguing for the expansion of data breach notification laws in light of IoT).

73. *See* Jay P. Kesan & Carol M. Hayes, *Liability for Data Injuries*, 2019 U. ILL. L. REV. 295, 343 ("The general rule forming from standing cases appears to be a preference for finding standing when there has at least been one incident of attempted fraud, whether that was a fraudulent credit card charge or a failed attempt to open a new credit account in the victim's name.").

74. Bradford C. Mank, *Data Breach, Identity Theft, and Article III Standing: Will the Supreme Court Resolve the Split in the Circuits?*, 92 NOTRE DAME L. REV. 1323, 1324–25 (2016) ("[T]he U.S. Supreme Court has interpreted Article III to impose mandatory standing requirements that require each plaintiff in federal court to demonstrate that he has suffered a concrete injury that is fairly traceable to the actions of the defendant and redressable by a favorable judgment of a federal court. . . . In data breach cases . . . the plaintiff cannot prove that a hacker or thief has actually used or sold the data to the plaintiff's detriment."); *see also In re* Zappos.com, Inc., 888 F.3d 1020, 1024 (9th Cir. 2018), *cert. denied*, 139 S. Ct. 1373 (2019) (denying a petition for certiorari seeking to resolve a circuit split on whether concrete injury is required to satisfy Article III standing).

75. U.S. CONST. art. III, § 2, cl. 1 ("The judicial Power shall extend to all Cases, in Law and Equity, arising under this Constitution, the Laws of the United States, and Treaties made, or which shall be made, under their Authority . . . to Controversies to which the United States shall be a Party;—to Controversies between two or more States;—between a State and Citizens of another State;—between Citizens of different States . . . .").

Supreme Court in *Spokeo v. Robins* interpreted the standing requirement as requiring the plaintiff to establish an "irreducible constitutional minimum" of, among other things, an "injury in fact."[76] In many circuits,[77] the injury-in-fact requirement has imposed serious limitations on remedies available to consumers whose personal information was compromised in a data breach.[78] The Supreme Court recently denied certiorari in a case seeking to resolve a circuit split over the question of standing in data breach litigation, in which courts disagree on whether a risk of future injury is sufficient to satisfy the standing requirement.[79] The question of harm in the context of availability attacks has not been fully addressed in case law.[80]

It remains to be seen whether Article III standing would affect litigation arising out of availability attacks, but it is likely that plaintiffs will have to establish that an availability attack caused them significant injury, though such an argument is not intuitive. For example, consumers filing a class-action lawsuit against a company which suffered a ransomware or DDoS attack due to negligence will have to prove actual, cognizable harm.[81] Additionally, the question of what constitutes "harm" is very much disputed.[82]

---

76. 136 S. Ct. 1540, 1547 (2016).

77. Priscilla Fasoro & Lauren Wiseman, *Standing Issues in Data Breach Litigation: An Overview*, INSIDE PRIV. (Dec. 7, 2018), https://www.insideprivacy.com/data-security/data-breaches/standing-issues-in-data-breach-litigation-an-overview (listing appellate court decisions on data breach standing).

78. *See* Luke Martin, *Resolving the Circuit Split on Article III Standing for Data Breach Suits*, COLUM. BUS. L. REV. ONLINE (Aug. 13, 2019), https://journals.library.columbia.edu/index.php/CBLR/announcement/view/181.

79. *See In re Zappos.com*, 888 F.3d at 1024.

80. *See, e.g.*, Fasoro & Wiseman, *supra* note 77.

81. *See id.*

82. *See generally* Daniel J. Solove & Danielle Keats Citron, *Risk and Anxiety: A Theory of Data-Breach Harms*, 96 TEX. L. REV. 737 (2018) (arguing that the law needs to recognize risk and anxiety as cognizable and redressable harms arising out of data breaches).

Overcoming the standing requirement may not necessarily guarantee a remedy.[83] As Rebecca Crootof explains, Internet of Things (IoT) manufacturers may be shielded from liability, including in a case involving an "implanted medical device [that] abruptly ceases to function,"[84] because "[e]xculpatory clauses limit civil remedies, IoT devices' bundled object/service nature thwarts implied warranty claims, and contractual notice of remote interference precludes common law tort suits."[85] Additionally, the fact that many devices nowadays are classified as "services" as opposed to "goods" may also contribute to a lack of effective remedy as implied warranty would be inapplicable.[86]

Third, the law creates an expectation that companies will invest predominately in the confidentiality aspect of information security. Companies are still likely to worry about integrity and availability attacks, but under the current state of cybersecurity law and its enforcement, they are most likely to face liability for incidents affecting the confidentiality of personal information.[87] If consumer information is compromised, the victim company is often liable if it was negligent in securing this information.[88] However, availability attacks do not raise similar liability under existing law. The law, therefore, is not sufficiently guiding companies on how to invest in the availability aspects of information security; neither does it currently provide any incentives to do so.

---

83. *See* Rebecca Crootof, *The Internet of Torts: Expanding Civil Liability Standards to Address Corporate Remote Interference*, 69 DUKE L.J. 583, 611–12 (2019).

84. *Id.* at 583.

85. *Id.*

86. *See In re* Sony Gaming Networks & Customer Data Sec. Breach Litig., 996 F. Supp. 2d 942, 983 (S.D. Cal. 2014) (dismissing plaintiff's warranty claims under Massachusetts's Uniform Commercial Code in data breach litigation against Sony—stemming from an attack on Sony PlayStation's Network that made it unavailable to users—because PlayStation Network was a "service" rather than "goods," and explaining that the Network is not a movable thing).

87. *See generally* Daniel J. Solove & Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, 114 COLUM. L. REV. 583 (2014) (discussing the FTC's focus on developing information privacy law).

88. *See* Sasha Romanosky et al., *Empirical Analysis of Data Breach Litigation*, 11 J. EMPIRICAL L. STUD. 74, 91 (2014) ("In this arena, dominated by class action practice . . . this translates to a higher probability of a federal lawsuit given evidence of actual financial loss, stronger claims of negligence (unauthorized disposal of information), and heightened protection of personal financial information.").

Fourth, cybersecurity law mandates public disclosure of data breaches.[89] State data breach notification statutes in all fifty states require companies to disclose to consumers any breaches impacting the confidentiality of certain types of personal information.[90] These statutes largely focus on the compromise of sensitive information, such as credit card numbers, Social Security numbers, addresses, driver license information, and more.[91] However, the same state data breach notification statutes are largely indifferent to breaches that affect the availability of systems and data.[92] After all, availability attacks do not directly compromise any sensitive information. Moreover, even if a breach does affect the confidentiality of personal information, statutes largely narrow down the types of compromised information that would require a breach notification.[93] This narrow scope of applicability may ignore a large chunk of cybersecurity incidents that consumers actually care about, including massive DDoS or ransomware attacks.

D. The Rise of Availability Attacks

The DDoS attack on Dyn demonstrated the ability of botnets to overwhelm a target with traffic to the point of unavailability.[94] With the rise of IoT, which is notoriously known to have weak security features,[95] DDoS attacks have become easier to execute and more

---

89. *See generally* BAKER HOSTETLER, DATA BREACH CHARTS (2018) (providing an overview of different state data breach notification statutes); FOLEY'S CYBERSECURITY TEAM, FOLEY & LARDNER LLP, STATE DATA BREACH NOTIFICATION LAWS (2020) (providing an overview of different state data breach notification statutes also).

90. *See Security Breach Notification Laws*, NAT'L CONF. STATE LEGISLATURES (July 17, 2020), https://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx.

91. *See generally* STEPTOE & JOHNSON LLP, COMPARISON OF US STATE AND FEDERAL SECURITY BREACH NOTIFICATION LAWS (2017).

92. *See* Mahmood Sher-Jan, *Is It an Incident or a Breach? How to Tell and Why It Matters*, IAPP (Feb. 28, 2017), https://iapp.org/news/a/is-it-an-incident-or-a-breach-how-to-tell-and-why-it-matters/ (categorizing cybersecurity occurrences in four categories, which may affect whether there is a reporting obligation: events, security incidents, privacy incidents, and data breaches).

93. *See, e.g.*, Sara Merken, *Washington State Enacts New Data Breach Notice Requirements*, BLOOMBERG L. (May 7, 2019, 4:56 PM), https://news.bloomberglaw.com/privacy-and-data-security/washington-state-enacts-new-data-breach-notice-requirements (reporting on Washington amending its data breach notification statute to expand the definition of "personal information").

94. Krebs, *supra* note 2.

95. *See, e.g.*, LAURA DENARDIS, THE INTERNET IN EVERYTHING: FREEDOM AND SECURITY IN A WORLD WITH NO OFF SWITCH 6–7 (2020).

devastating.[96] In particular, the volume of a DDoS attack nowadays can reach more than 1,000 gigabytes per second.[97] The devastation of availability attacks is expected to rise in an environment of potentially millions, and soon billions, of vulnerable devices,[98] which enable hackers to create enslaved IoT devices (botnets) that can be used as a proxy for attacking third parties.[99]

Similarly, ransomware attacks against critical sectors are becoming more common, and given the sensitive nature of the data encrypted, victims may have no choice but to pay the ransom, which consequently emboldens future attackers.[100]

Both DDoS and ransomware attacks reflect a trend in today's cybersecurity threat landscape.[101] Unlike confidentiality threats, which may result in loss and misuse of sensitive personal data at most, availability threats can have serious physical manifestations.[102] In a sense, cybersecurity law should become the law on consumer safety given how integrated smart devices have become in our daily lives.[103]

---

96. *See* Bruce Schneier, *Integrity and Availability Threats*, SCHNEIER ON SEC. (Jan. 29, 2016, 7:54 AM), https://www.schneier.com/blog/archives/2016/01/integrity_and_a.html ("It's one thing if your smart door lock can be eavesdropped to know who is home. It's another thing entirely if it can be hacked to prevent you from opening your door or allow a burglar to open the door.").

97. Liam Tung, *New World Record DDoS Attack Hits 1.7Tbps Days After Landmark GitHub Outage*, ZDNET (Mar. 6, 2018, 12:34 PM), https://www.zdnet.com/article/new-world-record-ddos-attack-hits-1-7tbps-days-after-landmark-github-outage.

98. Liam Tung, *IoT Devices Will Outnumber the World's Population This Year for the First Time*, ZDNET (Feb. 7, 2017, 12:24 PM), https://www.zdnet.com/ article/iot-devices-will-outnumber-the-worlds-population-this-year-for-the-first-time ("There will be 8.4 billion connected things in 2017, setting the stage for 20.4 billion Internet of Things (IoT) devices to be deployed by 2020, according to analyst firm Gartner.").

99. *See* Ido Kilovaty, *Freedom to Hack*, 80 OHIO STATE L.J. 455, 479 (2019).

100. *See, e.g.*, U.S. COMPUT. EMERGENCY READINESS TEAM, CYBERSECURITY & INFRASTRUCTURE SEC. AGENCY, RANSOMWARE: WHAT IT IS AND WHAT TO DO ABOUT IT, 1, 2, (n.d.) ("Ransomware is the fastest growing malware threat, targeting users of all types—from the home user to the corporate network. On average, more than 4,000 ransomware attacks have occurred daily since January 1, 2016. This is a [300%] increase over the approximately 1,000 attacks per day seen in 2015.").

101. Steve Ranger, *Ransomware, DDoS Now Top Threat as Hackers Look for Big Paydays*, ZDNET (Jan. 11, 2017, 12:37 PM), https://www.zdnet.com/article/ransomware-ddos-now-top-threats-as-hackers-look-for-big-paydays.

102. Greenberg, *supra* note 29; Lily Hay Newman, *A New Pacemaker Hack Puts Malware Directly on the Device*, WIRED (Aug. 9, 2018, 12:30 PM), https://www.wired.com/story/pacemaker-hack-malware-black-hat.

103. *See* Sean Michael Kerner, *Schneier: It's Time to Regulate IoT to Improve Cyber-Security*, SCHNEIER ON SEC. (Nov. 15, 2017), https://www.schneier.com/news/archives/2017/11/schneier_its_time_to.html ("'Availability and integrity threats

II. CYBERSECURITY LAW'S UNAVAILABILITY

If someone were to ask cybersecurity law "Why can't you just be normal?," cybersecurity law would likely just shriek back loudly.[104] Several theories account for the mismatch between information security and cybersecurity law.[105] This Part will review the patchwork of cybersecurity laws and then proceed to offer three theories as to why the mismatch between information security and cybersecurity law exists. The theories behind the mismatch may better inform the path forward.

A. Cybersecurity Law's Patchwork

Cybersecurity law is largely comprised of federal and state statutes and regulations that lack any coordination or consistency. In Jeff Kosseff's words, cybersecurity law is "an uncoordinated mishmash of requirements."[106] The categories of law that are largely understood to comprise cybersecurity law are: data security statutes,[107] data breach notification statutes, anti-hacking laws, and information-sharing laws. While this Article will not go into more detail, many would also include electronic surveillance laws[108] and common law pertaining to data breach litigation[109] within the scope of cybersecurity law.

---

are important as real risks to life and property now,' Schneier said. 'So now vulnerabilities have very different consequences, there is a difference between when a hacker crashes a computer and you lose your data and when a hacker hacks your car and then you lose your life.'").

104. *See Why Can't You Just Be Normal?*, KNOW YOUR MEME, https://knowyourmeme.com/memes/why-cant-you-just-be-normal (last visited Jan. 8, 2021).

105. *See supra* Part I.

106. *See* Kosseff, *supra* note 21, at 988.

107. Twenty-seven states currently have data security statutes. *See, e.g.*, CAL. CIV. CODE § 1798.81.5(b) (West 2020) ("A business that owns, licenses, or maintains personal information about a California resident shall implement and maintain reasonable security procedures and practices appropriate to the nature of the information.").

108. This primarily includes the Wiretap Act, 18 U.S.C. §§ 2510–2522 (2018), Stored Communications Act, 18 U.S.C. §§ 2701–2713 (2018), and the Pen Register Act, 18 U.S.C. §§ 3121–3127 (2018).

109. *See, e.g.*, Dittman v. UPMC, 196 A.3d 1036, 1056 (Penn. 2018) (holding that there is a common law duty for employers to safeguard their employees' personal information).

1. Data Security Statutes

Data security statutes generally set forth specific or general information security requirements for covered entities.[110] These statutes may be either sector-neutral or sector-specific (e.g., healthcare).[111] In theory, a comprehensive data security statute would cover all three threats: confidentiality, integrity, and availability.[112] Consider the healthcare sector, where the availability of health systems and information may be critical—a matter of life or death.[113] However, federal and state data security statutes often fail at their mission to offer guidelines to covered entities in securing against availability cybersecurity threats.

a. Section 5 of the Federal Trade Commission Act

Section 5 of the Federal Trade Commission Act empowers the FTC to investigate and pursue legal action against companies that engage in "unfair or deceptive acts or practices in or affecting commerce."[114] While cybersecurity and information security do not explicitly appear in the statute, the Third Circuit held in *FTC* v. *Wyndham Worldwide Corp.*,[115] that the FTC has authority under the "unfair" prong to regulate data security.[116] This is now largely the source of authority for the FTC to enforce data security regulations against companies whose practices are inadequate and result in harm to consumers; though, the Eleventh Circuit has scrutinized this authority as

---

110. *See, e.g.*, CAL. CIV. CODE § 1798.81.5(b) ("A business that owns, licenses, or maintains personal information about a California resident shall implement and maintain reasonable security procedures and practices appropriate to the nature of the information.").

111. *See id.* (discussing general security procedures with respect to personal information about California residents).

112. *See* Kosseff, *supra* note 21, at 997.

113. Jay P. Kesan & Carol M. Hayes, *Strengthening Cybersecurity with Cyberinsurance Markets and Better Risk Assessment*, 102 MINN. L. REV. 191, 193 (2017) ("[H]ackers have also targeted hospital computers with ransomware. Once a computer is infected, the ransomware locks hospital employees out of computers that hold vital information about patients—information that could literally be the difference between life and death—and demands payment to restore employees' access to the systems.").

114. 15 U.S.C. § 45(a)(1) (2018).

115. 799 F.3d 236, 240 (3d Cir. 2015) (affirming the district court's decision that the FTC has authority).

116. *Id.*

overbroad.[117] The FTC's authority is part of the cybersecurity law patchwork, which also includes as many as twenty-seven state data security statutes.[118] As the District of New Jersey in *Wyndham* acknowledged, the FTC's regulatory authority over data security may "coexist with the existing data security regulatory scheme."[119] Therefore, on the federal level, the FTC may pursue action against companies with data security practices that are deemed "unfair."[120]

It is unclear, however, how such unfairness is applied in the context of availability attacks.[121] If a company maintained that its services were hackproof, making any disruption impossible, then perhaps the FTC could initiate enforcement against that company if it suffered a DDoS or ransomware attack under its authority to prevent "deceptive acts or practices in or affecting commerce."[122] But because companies rarely deceptively claim they are unhackable, this kind of enforcement is unlikely.

But what about "unfair acts or practices"? While the FTC has been very active in using its data security authority against companies that failed at securing their customers' personal data, the FTC does not currently have a clear conception of how availability could be embedded in the unfairness standard. In 2015, the FTC published "Start with Security: A Guide for Business,"[123] which is often used to determine whether a data security practice would be unreasonable

---

117. LabMD, Inc. v. Fed. Trade Comm'n, 894 F.3d 1221, 1237 (11th Cir. 2018) (holding that the FTC must be very specific about what it means by "unfair or deceptive" with regard to data security).

118. JEFF KOSSEFF, CYBERSECURITY LAW 42 (2017) ("Twelve states have enacted statutes that impose data security requirements on companies that own or process personal information . . . ."). Though, an additional fifteen states have enacted their own statutes in recent years, bringing the total of states with data security statutes to twenty-seven.

119. Fed. Trade Comm'n v. Wyndham Worldwide Corp., 10 F. Supp. 3d 602, 613 (D.N.J. 2014).

120. *See id.*

121. *See* Norton Rose Fulbright, *FTC Enforcement Possible for Failing to Guard Against Ransomware*, DATA PROT. REP.: BLOG NETWORK (Oct. 6, 2016), https://www.dataprotectionreport.com/2016/10/ftc-enforcement-possible-for-failing-to-guard-against-ransomware (arguing that FTC enforcement is possible against companies that fail to patch vulnerabilities that allow ransomware attacks, though it is unclear if this will happen); *see also* Lesley Fair, *D-Link Case Alleges Inadequate Internet of Things Security Practices*, FED. TRADE COMM'N (Jan. 5, 2017), https://www.ftc.gov/news-events/blogs/business-blog/2017/01/d-link-case-alleges-inadequate-internet-things-security (summarizing the FTC suit against D-Link for inadequate security practices that, among other things, enabled DDoS attacks).

122. 15 U.S.C. § 45(a)(1) (2018).

123. *See generally* FED. TRADE COMM'N, START WITH SECURITY: A GUIDE FOR BUSINESS (2015) (covering basic technological vulnerabilities and tips to reduce risks).

and thus unfair, leading to FTC enforcement.[124] The Guide does not explicitly identify availability threats, nor does it offer any principles or guidelines for businesses to consider when implementing information security mechanisms. The Guide focuses on protecting the confidentiality of personal data.[125] Moreover, FTC enforcement actions are predominantly concerned with "(1) security of highly sensitive personal information, (2) security of payment card information, and (3) security violations that contradict privacy policies."[126]

In 2016, the FTC released a brief note containing tips on avoiding ransomware attacks.[127] While this note offered specific steps for businesses to implement to avoid becoming targets of ransomware,[128] it did little to shed light on whether the FTC would step in with enforcement actions should businesses fail to defend against ransomware attacks. This uncertainty is particularly alarming given that ransomware defies the traditional understanding of a cybersecurity threat.[129] While the FTC's responsiveness to trends in cybersecurity is noteworthy, especially given its critical staffing shortage,[130] more transparency and clarity is required as part of a more systemic response to availability attacks.

---

124. William R. Denny, *Cybersecurity as an Unfair Practice: FTC Enforcement Under Section 5 of the FTC Act*, AM. BAR ASS'N (June 20, 2016), https://www.americanbar.org/groups/business_law/publications/blt/2016/06/cyber_center_denny ("Wyndham moved to dismiss the complaint on the bases that . . . the 'unfairness' prong of Section 5 of the FTC Act did not encompass unreasonable data security measures . . . . In *FTC v. Wyndham Worldwide Corp.*, . . . the Third Circuit affirmed that the FTC has authority to regulate cybersecurity.").

125. FED. TRADE COMM'N, *supra* note 123, at 1.

126. *See* KOSSEFF, *supra* note 118, at 16.

127. Ben Rossen, *Ransomware – A Closer Look*, FED. TRADE COMM'N (Nov. 10, 2016), https://www.ftc.gov/news-events/blogs/business-blog/2016/11/ransomware-closer-look.

128. *Id.*

129. Malcolm Harkins & Anthony M. Freed, *The Ransomware Assault on the Healthcare Sector*, 6 J.L. & CYBER WARFARE 148, 148 (2018) ("The gamechanger with ransomware is the very real threat of data destruction, whereas before, malware may have been used to steal sensitive data that is ostensibly still accessible by the victim.").

130. Harper Neidig, *FTC Says It Only Has 40 Employees Overseeing Privacy and Data Security*, HILL (Apr. 3, 2019, 11:01 AM), https://thehill.com/policy/technology/437133-ftc-says-it-only-has-40-employees-overseeing-privacy-and-data-security.

b. Sector-specific Federal Data Security Statutes

In addition to the FTC's general data security authority, there are certain specific federal statutes that address data security for specific sectors. The Health Insurance Portability and Accountability Act (HIPAA),[131] applicable to the healthcare sector, and the Gramm-Leach-Bliley Act (GLBA),[132] applicable to the financial sector, are two such examples.

HIPAA, enacted in 1996, requires that the Secretary of Health and Human Services (HHS) create standards and regulations for healthcare cybersecurity.[133] In February 2003, HHS released what has become known as the "HIPAA Security Rule," which details the security safeguards required of the healthcare entities covered by HIPAA.[134] In its background, the HIPAA Security Rule seeks to "adopt national standards for safeguards to protect the confidentiality, integrity, and availability of electronic protected health information."[135]

Under the HIPAA Security Rule, a covered entity or business associate is obliged to report a breach in the case of a ransomware infection.[136] The HIPAA Security Rule defines a breach as "the acquisition, access, use, or disclosure of protected health information [PHI]."[137] Therefore, a ransomware attack could be viewed as an "acquisition" which mandates a breach notification.[138] While this interpretation is more expansive than other breach notification statutes, it says little about DDoS and other emerging availability attacks.

---

131. 42 U.S.C. § 1320d-2(d) (2018).

132. 15 U.S.C. §§ 6801–6809, 6821–6827 (2018).

133. 42 U.S.C. § 1320d-2(d)(1) (2018).

134. 45 C.F.R. § 164.104 (2011) (noting that the HIPAA security rule applies to "(1) a health plan[,] (2) a health care clearinghouse[,] [and] (3) a health care provider who transmits any health information in electronic form").

135. Health Insurance Reform: Security Standards, 68 Fed. Reg. 8,334 (Feb. 20, 2003) (to be codified at 45 C.F.R. pt. 160, 162, 164).

136. *See* DEP'T HEALTH & HUM. SERVS., FACT SHEET: RANSOMWARE AND HIPAA 4 (n.d.).

137. 45 C.F.R. § 164.402 (2011).

138. *See* DEP'T HEALTH & HUM. SERVS., *supra* note 136, at 5–6.

c. State Data Security Statutes

At present, twenty-seven states have enacted data security statutes.[139] These statutes generally require that companies either implement "reasonable security procedures,"[140] or, in four of the statutes, implement specific data security safeguards.[141]

There are two systemic problems with the current landscape of state data security statutes. First, those statutes that require "reasonable security procedures" often do so with the protection of the confidentiality and integrity of personal information in mind.[142] Consider, for example, the language of the California data security statute, requiring "reasonable security procedures and practices appropriate to the nature of the [personal] information, to protect the personal information from unauthorized access, destruction, use, modification, or disclosure."[143] This language suggests a strong confidentiality and integrity mindset[144] while ignoring the availability threat entirely. Moreover, the focus of these statutes is largely on personal information[145] while there may be nonpersonal information that is nonetheless valuable and the availability of which to the public is essential.

Second, the reasonableness standard is naturally ambiguous, and this ambiguity can be beneficial to stymying availability threats if interpreted liberally but can also increase uncertainty as to the specific safeguards for availability required by the respective statute.[146] This problem is, in fact, similar in nature to the FTC's data

---

139. *See, e.g.*, ARK. CODE ANN. § 4-110-104 (2019); CAL. CIV. CODE § 1798.81.5 (West 2009 & Supp. 2020); CONN. GEN. STAT. § 42-471 (2012 & Supp. 2020); FLA. STAT. § 501.171 (2016 & Supp. 2019); IND. CODE § 24-4.9-3-3.5 (2018); MD. CODE ANN., COM. LAW § 14-3503 (West 2020); TEX. BUS. & COM. CODE ANN. § 521.052 (West 2020)); UTAH CODE ANN. § 13-44-201 (West 2010); *see also Data Security Laws, Private Sector*, NAT'L CONF. STATE LEGISLATURES (MAY 29, 2019), https://www.ncsl.org/research/telecommunications-and-information-technology/data-security-laws.aspx (outlining states' data security statutes).

140. *E.g.*, ARK. CODE ANN. § 4-110-104(b) (2019).

141. The four states with specific data security statutes are Massachusetts, Nevada, Oregon, and Rhode Island. *See* MASS. GEN. LAWS ch. 93H, § 2(a) (2020); NEV. REV. STAT. § 603A.21 (2020); OR. REV. STAT. § 646A.622 (2011); 11 R.I. GEN. LAWS § 11-49.3-2(a) (Supp. 2020)).

142. *See, e.g.*, CAL. CIV. CODE § 1798.81.5.

143. *Id.* § 1798.81.5(c).

144. *See id.*

145. *See, e.g., id.*

146. Deal, *supra* note 69, at 2243 (arguing that the FTC had not provided companies with satisfactory guidance on the meaning of "reasonable" data security).

security authority under the unfairness prong, which often relies on a reasonableness standard.[147]

On the bright side, state data security statutes that mandate specific security procedures may hold more promise when it comes to defending against availability attacks. For example, the Rhode Island data security statute requires the same "reasonable security procedures and practices . . . to preserve the confidentiality, integrity, and *availability*"[148] of personal information. Unfortunately, Rhode Island's data security statute is not currently representative of other data security statutes, which tend to ignore availability threats.[149]

2. Data Breach Notification Statutes

Data breach notification law represents a patchwork of federal and state statutes that seek to impose a duty to notify affected individuals when their personal information has been compromised.[150] When a system is breached, the breached entity is required to send out notifications to consumers in accordance with the different state data breach notification laws.[151] By requiring breached entities to inform consumers, the law enables those affected to mitigate the associated risks by pursuing the course of action they deem appropriate or necessary.[152] Creating that sort of public awareness is immensely important in an area where secrecy and ambiguity in information security often prevail.

Data breach notification laws typically do not apply in cases of availability attacks because availability attacks do not expose the personal information on which data breach notification statutes

---

147. McGeveran, *supra* note 37, at 1149, 1176.

148. 11 R.I. GEN. LAWS § 11-49.3-2(a) (Supp. 2020) (emphasis added).

149. *See, e.g.*, CONN. GEN. STAT. § 42-471 (2012 & Supp. 2020); FLA. STAT. § 501.171 (2016 & Supp. 2019); MD. CODE ANN., COM. LAW § 14-3503 (West 2020).

150. *See* Sara A. Needles, *The Data Game: Learning to Love State-Based Approach to Data Breach Notification Law*, 88 N.C. L. REV. 267, 272, 293 (2009) (noting that federal data-breach notification law includes statutes like HIPAA and the Gramm-Leach-Bliley Act; further noting that state data-breach notification law includes all state statutes on the mandatory disclosure of a data breach affecting state residents); *see also* Karl D. Belgum, *Who Leads at Half-Time?: Three Conflicting Visions of Internet Privacy Policy*, 6 RICH. J.L. & TECH. 1, ¶ 24 (1999) (supporting the "disorganized patchwork" theory of regulatory schemes in the U.S.).

151. *See, e.g.*, Ido Kilovaty, *Data Breach Through Social Engineering*, HARV. L. REV. BLOG (Mar. 21, 2018), https://blog.harvardlawreview.org/data-breach-through-social-engineering.

152. *See* Needles, *supra* note 150, at 288.

typically rely.[153] If a system experiences an incident that significantly affects its availability to authorized users, the law does not mandate any form of disclosure.[154] This could create a transparency shortcoming and make companies less accountable to their consumers.

In the case of ransomware, for example, where personal information is encrypted until the victim pays the ransom, data breach notification law does not typically mandate public disclosure.[155] HHS distinguishes ransomware from other data breaches by noting that "its defining characteristic is that it attempts to deny access to a user's data . . . ."[156] While HIPAA would require data breach notification in the case of ransomware infecting a healthcare entity, general data breach notification laws do not, primarily because attackers do not take any personal information.[157]

Data breach notification laws, therefore, are often unable to address availability attacks, leaving consumers uninformed and helpless. The current focus of data breach notification law on the confidentiality, and sometimes integrity, of personal information is misguided in that it misses the importance of keeping consumers informed about disruptions that may affect their access to critical information technology resources.

3. Anti-hacking Laws

Availability attacks happen to be a concern of current anti-hacking laws far more than other components of cybersecurity law. On the federal level, the CFAA makes it an offense to "knowingly cause[] the transmission of a program, information, code, or command, and as a result of such conduct, intentionally cause[] damage without authorization, to a protected computer."[158] In that context, damage means "any impairment to the integrity or availability of data, a program, a system, or information."[159] While the

---

153. *See* LATHAM & WATKINS, RANSOMWARE ATTACKS: WHEN IS NOTIFICATION REQUIRED? 2 (2017).

154. *See id.* (noting that currently only HHS has issued explicit guidelines for requiring ransomware attack disclosure).

155. *Id.*

156. DEP'T HEALTH & HUM. SERVS., *supra* note 136, at 1.

157. LATHAM & WATKINS, *supra* note 153, at 3.

158. 18 U.S.C. § 1030(a)(5)(A) (2018).

159. *Id.* § 1030(e)(8).

CFAA is not without problems,[160] it treats availability attacks in a manner unprecedented in other cybersecurity statutes, punishing offenders[161] who mount DDoS, ransomware, or any other availability attacks against "protected computers."[162] Indeed, the Department of Justice is very active in prosecuting DDoS offenses.[163]

The CFAA also establishes a private cause of action, for example, in cases where damages reach at least $5,000 in one year[164] or if an offense causes physical injury to any person.[165] This civil suit may be used by victims against offenders who carry out availability attacks, offering an ex-post compensation against such attacks.[166] However, it is worth noting that a civil cause of action is only available to the immediate victim and not necessarily to those who may suffer from the unavailability of critical computers, networks, and data.[167]

While CFAA seems to have some promise with regard to availability attacks, it is only one piece of the cybersecurity law puzzle. To more effectively prevent availability attacks through regulatory compliance and to ensure that consumers are informed

---

160. *See, e.g.*, Orin S. Kerr, *Vagueness Challenges to the Computer Fraud and Abuse Act*, 94 MINN. L. REV. 1561, 1562, 1572 (2010) (arguing that the CFAA has become too broad, which could potentially invoke a vagueness challenge).

161. *See* 18 U.S.C. § 1030(c) (punishing offenders of the statute by either fine or imprisonment for up to twenty years).

162. "Protected computer" is a term interpreted very broadly under the CFAA and may virtually encompass every computer in the United States (and sometimes abroad):

> [T]he term "protected computer" means a computer—
> (A) exclusively for the use of a financial institution or the United States Government, or, in the case of a computer not exclusively for such use, used by or for a financial institution or the United States Government and the conduct constituting the offense affects that use by or for the financial institution or the Government; or
> (B) which is used in or affecting interstate or foreign commerce or communication, including a computer located outside the United States that is used in a manner that affects interstate or foreign commerce or communication of the United States.

See id. § 1030(e)(2)

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

164. 18 U.S.C. § 1030(c)(4)(A)(i)(I).

165. *Id.* § 1030(c)(4)(A)(i)(III).

166. *See id.* § 1030(g).

167. *See id.*

about such attacks and their consequences, cybersecurity law is in dire need of reform.

4. Information Sharing

Cybersecurity law also creates legal mechanisms for information sharing with regard to cybersecurity threats. This typically involves private entities sharing this information with government entities and vice versa. The Cybersecurity Information Sharing Act (CISA) of 2015 is an example of a statute creating this information-sharing mechanism.[168] The statute encourages entities to monitor their systems for cybersecurity purposes in exchange for limited liability under the Electronic Communications Privacy Act.[169] CISA defines a "cybersecurity threat" rather broadly, as:

> [A]n 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.[170]

This definition, which includes availability, allows private entities to share information regarding cybersecurity threats among themselves without facing antirust liability.[171] However, while this broad definition may promote information sharing with regard to availability attacks and is certainly important, it only represents a small subset of cybersecurity law.

B. Explaining the Patchwork and the Mismatch

This Article offers three theories to explain the reasons behind the current patchwork of cybersecurity law and the mismatch between information security and cybersecurity law.

---

168. 6 U.S.C. § 1502 (2018).
169. *Id.* §§ 1501(13), 1503(a)–(b), 1505.
170. *Id.* § 1501(5)(A).
171. *Id.* § 1505(b).

1. Cybersecurity Law Is Based on Outdated Paradigms

Cybersecurity law is largely a patchwork of federal and state statutes and regulations that lack any cohesiveness.[172] Statutes and regulations are often enacted to address discrete cybersecurity shortcomings without due regard to a broader cybersecurity strategy.[173] As Andrea Matwyshyn argues, these statutes largely adopt dated paradigms of information sharing and deterrence.[174] Information sharing focuses on information security data shared between the private and public sector[175] while deterrence seeks to coerce relevant actors into complying with certain rules,[176] whether regulatory or criminal.

These two paradigms are problematic in today's information security landscape because they miss the broader shortcomings that involve shared vulnerabilities between the private and public sectors.[177] Matwyshyn refers to this as the "reciprocal security vulnerability," meaning that "security flaws and vulnerabilities in the private sector impact the public sector and vice versa."[178] The Government Accountability Office acknowledged the same concern when it admitted that the internet is controlled by a variety of actors, each with their own standards and procedures.[179] Neither information sharing nor deterrence addresses the problem of shared

---

172. *See* Kosseff, *supra* note 58, at 157 ("Cybersecurity regulation is determined by more than [7,000] state legislators, and it is enforced by fifty governors and fifty state attorneys general and their staffs. This bouillabaisse of state cybersecurity laws makes it impossible for the United States to develop a cohesive strategy to secure itself from increasingly persistent and advanced cyber threats. Although new cybersecurity threats emerge daily, many state cybersecurity laws are more than a decade old and have not changed.").

173. J.M. Porup, *Georgia Governor Vetoes Bill that Would Criminalize Good-Faith Security Research, Permit Vigilante Action*, CSO ONLINE (May 8, 2018, 1:25 PM), https://www.csoonline.com/article/3269206/new-georgia-law-criminalizes-good-faith-security-research-permits-vigilante-action.html (reporting that Georgia's governor vetoed a bill that would have criminalized good-faith cybersecurity research, which was vehemently criticized by the information security community).

174. *See* Matwyshyn, *supra* note 20, at 1125–26.

175. *Id.* at 1128.

176. *Id.* at 1129.

177. *See id.* at 1127.

178. Andrea M. Matwyshyn, *Cyber Harder*, 24 B.U. J. SCI. & TECH. L. 450, 453 (2018).

179. U.S. GOV'T ACCOUNTABILITY OFF., GAO-06-672, INTERNET INFRASTRUCTURE: DHS FACES CHALLENGES IN DEVELOPING A JOINT PUBLIC/PRIVATE RECOVERY PLAN 37 (2006).

vulnerability,[180] and thus, they cannot effectively address the availability attacks these vulnerabilities enable.

The focus of cybersecurity law, therefore, ought to be patching software vulnerabilities both in the public and private sectors. Ransomware attacks, as well as other availability attacks, proliferate because they take advantage of existing software vulnerabilities.[181] Patching these and providing the incentives to identify them is the key to a robust approach to availability threats.[182]

Moreover, certain statutes are often over a decade old, which strengthens the view that these paradigms are outdated, especially in the fast-moving threat landscape of information security.[183] This may explain why there is little cybersecurity law that applies across the United States and why states have divergent legal landscapes when it comes to cybersecurity.

2. Tension Between Cybersecurity Law and Innovation

The second theory focuses on the uneasy relationship between innovation and regulation more generally, which is equally applicable to cybersecurity law. The argument goes that the tech sector wants to innovate while cybersecurity regulation adds complexity, time, and cost and thus stifles innovation.[184] Under this theory, existing cybersecurity law is suboptimal because it developed with the view of not stifling technological innovation, which inevitably excludes certain information security threats from its scope.[185] Regulation is

---

180. Matwyshyn, *supra* note 20, at 1126–27.

181. *See, e.g.*, Schneier, *supra* note 34.

182. *See* Matwyshyn, *supra* note 20, at 1121 ("[W]e need to fix all the vulnerable systems in both the public and the private sector because the compromise of either could potentially lead to compromise of both." (emphasis omitted)).

183. *See* Kosseff, *supra* note 58, at 157.

184. *See* NAT'L RSCH. COUNCIL OF THE NAT'L ACADS., AT THE NEXUS OF CYBERSECURITY AND PUBLIC POLICY: SOME BASIC CONCEPTS AND ISSUES 98 (David Clark et al. eds., 2014) ("Policy actions that detract from the ability of the private sector to innovate are inherently suspect from this perspective, and in particular policy actions to promote greater attention to cybersecurity in the private sector often run up against concerns that these actions will reduce innovation. The logic of reducing time to market for information technology products or services runs counter to enhancing security, which adds complexity, time, and cost in design and testing while being hard to value by customers.").

185. Claudia Ng, *Regulating Fintech: Addressing Challenges in Cybersecurity and Data Privacy*, GOV'T INNOVATORS NETWORK BLOG (Feb. 22, 2018), https://www.innovations.harvard.edu/blog/regulating-fintech-addressing-challenges-cybersecurity-and-data-privacy ("Regulators are experimenting with tools to oversee

largely seen as a burden and cost for innovators to consider and could decrease overall competitiveness and disincentivize technological innovation.[186]

As a result, any existing information security regulation is the result of a balance between the benefits of unregulated innovation and potential harm to consumers from cybersecurity incidents.[187] This has led to regulation addressing very specific sectors and information security concerns, often to the exclusion of availability threats.

On the other hand, some research suggests that it may be the other way around—that regulation promotes innovation in the information security industry.[188] The reality is likely somewhere in between these two views. Regulators avoid overregulating, and when they do regulate, the information security industry has an incentive to innovate while other tech industries may have a perverse incentive to innovate to avoid liability under cybersecurity law. In addition, even if regulation stifles some innovation, innovation should not be a trump card as there are often other interests and values at stake.[189] In light of the growing threat landscape of availability attacks, it is time to recalibrate cybersecurity regulation.

3. Today's Availability Attacks Are Different

Third, cybersecurity law developed at a time when availability attacks were not as concerning as they are now and will likely be in the very near future.[190] As Kosseff explains, most U.S. cybersecurity

---

this new [Fintech] industry to ensure customer protection and cybersecurity without stifling innovation.").

186. *See* NAT'L RSCH. COUNCIL OF THE NAT'L ACADS., *supra* note 184, at 98.

187. F. Patrick Hubbard, *"Sophisticated Robots": Balancing Liability, Regulation, and Innovation*, 66 FLA. L. REV. 1803, 1811 (2014).

188. Lara Khansa & Divakaran Liginlal, *The Influence of Regulations on Innovation in Information Security*, AM. CONF. INFO. SYS., Dec. 2007 at 1, 1 ("We postulate that regulatory compliance pressures that have forced information security out of obscurity and into the corporate boardroom provide economic justification for information security firms to innovate. We aim to establish the link between regulations and innovation through the intermediary of demand for information security products and services.").

189. Yafit Lev-Aretz & Katherine J. Strandburg, Better Together: Privacy Regulations and Innovation Policy 7 (Feb. 15, 2019) (unpublished manuscript) (available at https://www.law.nyu.edu/sites/default/files/Lev-Aretz%20AND%20Strandburg.pdf) ("'[I]nnovation' in some vague sense is not a trump card outweighing all other social benefits. Of course, particular regulations might have deleterious effects on innovation that outweigh their benefits. The point is that the devil is largely in the details.").

190. *See* Crootof, *supra* note 83, at 589.

law is based on "century-old privacy norms, torts, and criminal laws" that look nothing like the concerns of information security.[191] With the permeation of the internet in every aspect of our lives, including through the proliferation of IoT, availability attacks may have far-reaching and devastating consequences that cybersecurity law, with the exception of the U.S. Congress[192] and California,[193] has thus far failed to consider.

For example, while Denial of Service attacks are not new per se, their ability to be distributed (involving more than one attacker) and amplified (requesting response from the victim to each communication) is more devastating than ever.[194] In other words, availability attacks are not novel, but their power to extort and disable victims is.

Additionally, consider ransomware attacks. The introduction of cryptocurrencies, some of which are valued at thousands of dollars per unit, enabled the proliferation of these extortion cyberattacks, which encrypt valuable data in exchange for a cryptocurrency transfer.[195] The examples of DDoS and ransomware reflect the evolution that availability attacks have undergone in recent years. The law has failed to take these into full consideration.

It is likely that a combination of the aforementioned three theories is the predominant reason why cybersecurity law fails to address

---

191. *See* Kosseff, *supra* note 21, at 988.

192. Alfred Ng, *Congress Introduces Bill to Improve 'Internet of Things' Security*, CNET (Mar. 11, 2019, 12:42 PM), https://www.cnet.com/news/congress-introduces-bill-to-improve-internet-of-things-security ("There's no national standard for IoT security and it's up to each company to decide how secure they want to make their connected devices. Lawmakers are looking to fix that with the bill, which would require a bare minimum of security standards for any IoT devices that the federal government uses.").

193. Adi Robertson, *California Just Became the First State with an Internet of Things Cybersecurity Law*, VERGE (Sept. 28, 2018, 6:07 PM), https://www.theverge.com/2018/9/28/17874768/california-iot-smart-device-cyber security-bill-sb-327-signed-law (reporting that the bill requires device manufacturers to implement reasonable security features to prevent unauthorized access, modification, or information disclosure, but noting that experts criticized the bill for being too vague or not going far enough).

194. *DNS Amplification Attack*, CLOUDFLARE, https://www.cloudflare.com/learning/ddos/dns-amplification-ddos-attack (last visited Oct. 22, 2020).

195. Brian Fung, *What You Need to Know About Bitcoin After the WannaCry Ransomware Attack*, WASHINGTON POST (May. 15, 2017, 3:42 PM), https://www.washingtonpost.com/news/the-switch/wp/2017/05/15/what-you-need-to-know-about-bitcoin-after-the-wannacry-ransomware-attack; Nathaniel Popper, *Bitcoin Has Lost Steam. But Criminals Still Love It.*, N.Y. TIMES (Jan. 28, 2020), https://www.nytimes.com/2020/01/28/technology/bitcoin-black-market.html.

availability attacks. This Article argues for the reimagination of cybersecurity law in light of its current inadequacy.

III. REIMAGINING CYBERSECURITY LAW

The unsatisfactory landscape of today's cybersecurity law calls for a reimagination of its guiding values. Cyberspace and new technologies challenge the notion that data confidentiality and integrity are the only important objectives of cybersecurity law.[196] The definition of "cybersecurity law," therefore, hinges on the harms it seeks to prevent.[197] Naturally, in the information security context, these harms evolve over time. The availability of computers, networks, and data can be framed as an issue of *human safety*, *national security*, and *infrastructure stability*.

A. Cybersecurity Law Is About Human Safety

In recent years, many scholars have alerted us that cybersecurity's priorities ought to change in light of the advent and mass adoption of certain technologies, such as IoT, particularly when used on or in human bodies.[198] Andrea Matwyshyn argues that IoT and artificial intelligence merge with the human body.[199] This reflects what Matwyshyn describes as the "platformization" of the human body,[200] which holds much promise but also introduces cybersecurity threats to humans' physical and mental wellbeing. For example, the compromise of a vulnerable smart pacemaker may cause significant bodily harm.[201]

Cybersecurity law, therefore, is not exclusively about the protection of sensitive information but also about the protection of

---

196. *See* John J. Chung, *Critical Infrastructure, Cybersecurity, and Market Failure*, 96 OR. L. REV. 441, 441 (2018) ("[W]hen most people think about cybersecurity and cyberattacks, their attention probably turns to privacy violations and theft of personal information.").

197. Kosseff, *supra* note 21, at 989.

198. *See* Andrea M. Matwyshyn, *Internet of Bodies*, 61 WM. & MARY L. REV. 77, 83 (2019).

199. *Id.* at 82.

200. *Id.*

201. *Id.*; *see also Cybersecurity Vulnerabilities Affecting Medtronic Implantable Cardiac Devices, Programmers, and Home Monitors: FDA Safety Communication*, *supra* note 32 (discussing the cybersecurity concerns and vulnerabilities posed by an IoT implanted cardiac device).

human safety; digital security *is* physical security.[202] If computerized devices will increasingly be embedded in our bodies, any potential compromise to their availability will result in significant bodily harm and potentially death.[203] Reframing cybersecurity law as a human safety issue will contribute to the development of better-informed statutes and regulations.

B. Cybersecurity Law Is About National Security

Compromises to the availability of computers, networks, and data can also be considered a national security concern in certain circumstances. President Obama himself noted that cybersecurity is "one of the most serious economic and national security challenges that we face as a nation."[204] The White House National Security Strategy has also been making direct references to cybersecurity as a national security priority.[205]

In 2014, North Korea attacked Sony in retaliation for making the movie "The Interview," which was centered around the assassination of North Korean leader Kim Jong Un.[206] Sony executives received phishing emails, which directed them to a fake Apple login screen. That way, hackers were able to obtain the credentials of Sony's top executives, allowing them to remotely access Sony's systems. While these credentials enabled the theft of sensitive information belonging to Sony, they also led to the destruction of data, disruption of Sony operations, and reputational harm.[207]

While the target might have been a private corporation, it is undisputed that this created a national security crisis.[208] President Obama, who was pressed to react to the incident, refused to call this

---

202. *See* Matwyshyn, *supra* note 178, at 453 ("[P]hysical security and digital security are inextricably interwoven.").

203. *See* Matwyshyn *supra* note 198, at 83 ("The August 2017 [IoT] pacemaker security recall was not, however, the first time that computer code put human bodies at risk of physical harm and death.").

204. Barack Obama, U.S. President, Remarks by the President at the Cybersecurity and Consumer Protection Summit (Feb. 13, 2015), (transcript available at https://obamawhitehouse.archives.gov/the-press-office/2015/02/13/ remarks-president-cybersecurity-and-consumer-protection-summit).

205. WHITE HOUSE, NATIONAL SECURITY STRATEGY OF THE UNITED STATES OF AMERICA 12–13 (2017).

206. Andrea Peterson, *The Sony Pictures Hack, Explained*, WASHINGTON POST (Dec. 18, 2014, 4:15 PM), https://www.washingtonpost.com/news/the-switch/wp/2014/12/18/the-sony-pictures-hack-explained.

207. *Id.*

208. *Id.*

an act of war, instead labeling the attack as "cyber-vandalism."[209] Given that cybersecurity incidents happen daily, it is unusual to see a president react to any single incident. However, the increasing nation-state involvement in cyberattacks against private corporations which cause availability issues reflects the notion that cybersecurity *is* about national security, among other things. Cybersecurity law that robustly addresses availability threats is also contributing to national security by making it less likely that availability attacks occur in the first place.

C. Cybersecurity Law Is About Infrastructure Stability

Furthermore, cybersecurity law's focus on availability attacks may also enhance the overall information security of infrastructure, such as energy, emergency services, healthcare, law enforcement, and more.[210]

Recently, nation states have become interested in targeting civilian infrastructure in cyberspace. Russia, for example, has recently successfully hacked the U.S. power grid.[211] Russia has similarly been involved in attacks against Ukraine that caused widespread blackouts.[212] This shows that the technology is already

---

209. Steven Holland & Doina Chiacu, *Obama Says Sony Hack Not an Act of War*, REUTERS (Dec. 21, 2014, 9:55 PM), https://www.reuters.com/article/us-sony-cybersecurity-usa/obama-says-sony-hack-not-an-act-of-war-idUSKBN0JX1MH20141222.

210. The Cybersecurity and Infrastructure Security Agency identifies "critical infrastructure" as the following sectors: chemical, commercial facilities, communications, critical manufacturing, dams, defense industrial base, emergency services, energy, financial services, food and agriculture, government facilities, healthcare and public health, information technology, nuclear reactors, materials, and waste, transportation systems, and water and wastewater. *See Critical Infrastructure Sectors*, CYBERSECURITY & INFRASTRUCTURE SEC. AGENCY, https://www.cisa.gov/critical-infrastructure-sectors (last updated Oct. 21, 2020); *see also* 42 U.S.C. § 5195c(b)(3) (2018) ("A continuous national effort is required to ensure the reliable provision of cyber and physical infrastructure services critical to maintaining the national defense, continuity of government, economic prosperity, and quality of life in the United States.").

211. Brian Naylor, *Russia Hacked U.S. Power Grid — So What Will the Trump Administration Do About It?*, NPR (Mar. 23, 2018, 5:00 AM), https://www.npr.org/2018/03/23/596044821/russia-hacked-u-s-power-grid-so-what-will-the-trump-administration-do-about-it.

212. Andy Greenberg, *How an Entire Nation Became Russia's Test Lab for Cyberwar*, WIRED (June 20, 2017, 6:00 AM), https://www.wired.com/story/russian-hackers-attack-ukraine; *see also* Kim Zetter, *Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid*, WIRED (Mar. 3, 2016, 7:00 AM),

there, and any compromise to the availability of infrastructure may have devastating consequences, such as widespread blackouts, unavailability of emergency services, and more.[213] Indeed, energy infrastructure is "probed thousands of times each month by hackers,"[214] which suggests that the phenomenon is likely to increase in scale and effect.

The energy sector is not the only victim of availability attacks against infrastructure. In 2017, the WannaCry ransomware was able to infect the healthcare sector in the United Kingdom by encrypting patient data and making it impossible for hospitals to function properly.[215] As many as 19,000 medical appointments had to be cancelled as a result.[216]

Cybersecurity law's role, therefore, ought to be to protect infrastructure through a robust approach toward dealing with availability threats. Infrastructure already widely relies on cyber-physical systems, so its dependency on the internet creates its vulnerability to availability attacks like ransomware and DDoS.[217] This realization needs to guide future cybersecurity law.

IV. AVAILABILITY'S LAW

Cybersecurity law needs to evolve in a manner that recognizes the need to deter, prevent, and respond to availability attacks. DDoS, ransomware, and other availability attacks should receive a more comprehensive treatment under the different parts of cybersecurity law. In addition, the emerging landscape of IoT must receive more attention, as it presents an attack vector that can facilitate availability attacks.[218]

---

https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid (arguing that Russian hackers might target U.S. infrastructure next).

213. *See* Zetter, *supra* note 212.

214. Chung, *supra* note 196, at 443.

215. Matthew Field, *WannaCry Cyber Attack Cost The NHS £92m as 19,000 Appointments Cancelled*, TELEGRAPH (Oct. 11, 2018, 6:05 PM), https://www.telegraph.co.uk/technology/2018/10/11/wannacry-cyber-attack-cost-nhs-92m-19000-appointments-cancelled.

216. *Id.*

217. *See* Chandler, *supra* note 51, at 239 ("Power grids, gas and oil distribution pipelines, water treatment and distribution systems, hydroelectric and flood control dams, oil and chemical refineries[,] and other infrastructures have long been controlled by computer through SCADA systems (supervisory control and data acquisition systems) and other networked computer systems. These control systems are now increasingly being connected to communications networks in order to lower costs by permitting remote maintenance, control[,] and updating.").

218. *See* Schneier, *supra* note 35.

This Part makes four proposals on how cybersecurity law should proceed with regard to availability attacks. First, all states' computer crime statutes should have CFAA-like offenses directed at availability attacks. At present, many states have not designated a specific criminal offense covering attackers who engage in DDoS or ransomware attacks within the confines of one state.[219] To be clear, amending criminal statutes to capture today's cybersecurity threats is not a panacea, and a broader approach is likely to prove more effective.[220]

Second, legislators should consider amending data breach notification statutes to better inform consumers about the occurrence of availability attacks. Currently, data breach notification laws apply narrowly to compromises of personal information.[221] Reducing the information gap between consumers and companies can ensure that consumers make informed choices and are aware of any interferences with the availability of services they use.

Third, the definition of "reasonable security practices" should grow to include the practice of using mitigation tools for availability attacks. This revised meaning would inform enforcement activity by the FTC and other entities as they pursue action against companies who do not practice reasonable security standards to prevent availability attacks.

Fourth, legislation addressing availability threats will be needed in the near future. As availability attacks become more devastating, the enactment of specific legislation mandating certain tools and procedures to reduce their likelihood and impact will be required. For example, legislation on minimal security standards for IoT may improve overall information security as it pertains to availability threats.

A. Harmonizing Computer Crime Statutes

While the CFAA makes it an offense to transmit a "program, information, code, or command"[222] which impairs the "availability of

---

219. *See* JAY P. KESAN & CAROL M. HAYES, CYBERSECURITY AND PRIVACY LAW IN A NUTSHELL 75 (2019).

220. *See* Jeff Kosseff, *Positive Cybersecurity Law: Creating a Consistent and Incentive-Based System*, 19 CHAP. L. REV. 401, 418 (2016) (calling for more cooperation between the private and public sectors in cybersecurity).

221. *See, e.g.*, Jeff Kosseff, *Cybersecurity of the Person*, 17 FIRST AMENDMENT L. REV. 343, 345 (2018) (arguing that our current conception of data breach notification is too narrowly applied).

222. 18 U.S.C. § 1030(a)(5)(A) (2018).

data, a program, a system, or information,"[223] there is far less uniformity on the matter in state computer crime statutes. At present, only thirty state statutes make it a crime to disrupt a system or cause denial of service.[224] While this type of criminal offense may deter DDoS attacks, it says little about other disruptive availability attacks, such as ransomware or whatever new techniques hackers will devise.

While most state computer crime statutes do not explicitly address ransomware, five states currently proscribe the use of encryption related to committing a criminal offense.[225] The Virginia computer crime statute, for example, makes it a criminal offense to use "encryption to further any criminal activity."[226] While this may deter hackers who use ransomware attacks for financial gain, the scope of application of these statutes is still limited to the states where such use of encryption is proscribed.[227]

When it comes to harmonization, cybersecurity law needs to be mindful of two inconsistencies.

First, there is often a mismatch between state and federal cybersecurity law.[228] Some activity is outlawed by federal cybersecurity law, whereas the same activity would not be considered a crime under certain state laws. There is no good reason for states not to have an equivalent criminal offense if the act is committed entirely within the confines of a single state.

Second, federal law's sector-by-sector approach introduces significant gaps when applied to new technologies that defy existing categories and definitions.[229] For example, HIPAA applies *only* in the healthcare sector, but other sectors may nonetheless pose significant health risks to individuals if compromised through an availability attack. For example, private genetic testing companies are not considered to be "covered entities" under HIPAA, and they represent

---

223. *Id.* § 1030(e)(8).

224. KESAN & HAYES, *supra* note 219, at 75.

225. *Id.* at 87.

226. VA. CODE ANN. § 18.2-152.15 (2020).

227. *See id.*

228. *Compare* 18 U.S.C. § 1030(a)(5)(A) (making it an offense to transmit a "program, information, code, or command"), *with* VA. CODE ANN. § 18.2-152.15 (criminalizing encryption that furthers any criminal activity).

229. *See, e.g.*, Nuala O'Connor, *Reforming the U.S. Approach to Data Protection and Privacy*, COUNCIL ON FOREIGN RELS. (Jan. 30, 2018), https://www.cfr.org/report/reforming-us-approach-data-protection ("[T]he law should harmonize the inconsistencies and fill the gaps created by the existing sectoral approach. Health information is sensitive regardless of whether it is input into a consumer application, generated by a wearable device, or conveyed to a medical professional.").

but one example out of an ever-growing subset of private companies that increasingly work with health data.[230]

Regulation of information security through coercion and deterrence is not a silver-bullet solution, however.[231] It must be part of a broader strategy to address the current underlying problems, as discussed below.

B. Disclosure of Availability Attacks

At present, there is no general federal data breach notification statute.[232] State data breach notification statutes apply exclusively in cases compromising personal information, with varying definitions.[233] However, by applying solely to data breaches that compromise personal information, data breach notification statutes only focus on the confidentiality aspect of cybersecurity.[234] Data breach notification law can do more in the context of availability.

Jeff Kosseff, in his article *Cybersecurity of the Person*, has argued that our current conception of data breach notification is misguided because it too narrowly focuses on financial harms arising from the compromise of personal information.[235] A similar argument has been made about the need to apply data breach notification law to cases where data breaches cause harms to dignity[236] or are used in

---

230. *See Genetic Information Privacy*, ELEC. FRONTIER FOUND., https://www.eff.org/issues/genetic-information-privacy (last visited Oct. 22, 2020).

231. *See* Kosseff, *supra* note 21, at 1003 ("A unilateral focus on coercion through regulation would be misguided, as there are many opportunities for cooperative cybersecurity law.").

232. Rachel German, *What Are the Chances for a Federal Breach Notification Law?*, UNIV. OF TEX. AUSTIN CTR. FOR IDENTITY (Apr. 14, 2015), https://identity.utexas.edu/id-experts-blog/what-are-the-chances-for-a-federal-breach-notification-law [https://web.archive.org/web/20200206143140/https://identity.utexas.edu/id-experts-blog/what-are-the-chances-for-a-federal-breach-notification-law].

233. *See, e.g.*, CAL. CIV. CODE § 1798.82(a) (West 2020) ("[P]erson or business that conducts business in California, and that owns or licenses computerized data that includes personal information, shall disclose a breach of the security of the system following discovery or notification of the breach in the security of the data to a resident of California (1) whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person . . . ."). Personal information often includes Social Security numbers, driver's license and ID numbers, and account or credit and debit card numbers.

234. *See id.*

235. Kosseff, *supra* note 221, at 343.

236. George Ashenmacher, *Indignity: Redefining the Harm Caused by Data Breaches*, 51 WAKE FOREST L. REV. 1, 5–6 (2016) ("But have individuals been harmed even where their [personally identifiable information] has not been used to commit fraud? . . . By and large, American law has responded with an unsympathetic 'no.'").

furtherance of manipulation.[237] Along similar lines, this Article argues that data breach notification law may have a role in informing consumers about the occurrence of availability attacks affecting the accessibility of systems and data.

While data-breach notification law is primarily concerned with the prevention of identity theft as a result of unauthorized acquisition of personal information, this law protects a variety of other interests in practice, whether intentionally or inadvertently.[238] These interests include reducing risk and uncertainty and bridging the information gap between firms and consumers.[239]

It therefore follows that the disclosure of availability compromises to the public and regulators may serve three important purposes. First, consumers would be better informed about the cybersecurity practices of companies with whom they have transactional relationships and the degree of reliability of the services offered by these companies. Second, regulators would be aware of any availability attacks affecting access to systems, networks, and data. Because many availability attacks are unreported to the public, this may change the status quo and increase transparency and consumer freedom of choice. Third, mandatory disclosure to consumers and reporting to authorities may create more data about trends in availability attacks, which may later inform policy and law.

Currently, when a data breach increases the risk of identity theft for consumers, the law typically requires that the breached company notify its consumers.[240] After all, the company in question has direct access to breach-related information that could help consumers reduce the risk of identity theft. The same company would have direct access to information pertaining to attacks that have affected the availability of its systems and data and the consequences of such attacks.

---

237. Ido Kilovaty, *Legally Cognizable Manipulation*, 34 BERKELEY TECH. L.J. 449, 456, 470 (2019).

238. *See* Needles, *supra* note 150, at 270–71 ("More than simply combating identity theft and economic harm to individuals, many state data breach notification laws strike a balance between the conflicting effects on consumers and businesses. Analyzing what a breach notification portends implicates these two main parties that, in terms of privacy interests, are at odds with one another. Business interests in monetizing data clash against consumer protection groups' cry for data privacy.").

239. *See id.*

240. *See* KOSSEFF, *supra* note 118, at 39–40 ("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 [identity theft or fraud] harm for individuals whose personal information was exposed.").

A 2016 RAND study supports the fact that consumers expect to be notified.[241] In this study, titled "Consumer Attitudes Toward Data Breach Notification and Loss of Personal Information," RAND explored a series of questions relating to consumers' perception and experience of data breaches affecting them.[242] The study asked respondents of the manner in which they learned about a data breach.[243] As many as 56% of respondents first learned of a breach by receiving a notification from the affected company.[244] This means that data breach notification is still a major factor in reducing information gaps between breached companies and their consumers, and it would be an important tool in notifying consumers about availability compromises.

The realization that some availability attacks may be notification-worthy has already been gaining traction.[245] North Carolina, for example, has introduced a bill that would classify ransomware attacks as data breaches, therefore making them reportable under North Carolina's data breach notification law.[246] Other states would be wise to follow suit and amend their data breach notification laws to incorporate emerging cybersecurity threats about which consumers would want to be notified.

C. FTC Enforcement and Market-based Tools

A lot has been written on the FTC's role in enforcing reasonable data security practices.[247] While the FTC is an important and essential actor in the enforcement of cybersecurity law, its focus to date has been largely on cybersecurity incidents affecting the confidentiality of consumer personal information.[248] In *FTC v.*

---

241. *See* LILIAN ABLON, ET AL., CONSUMER ATTITUDES TOWARD DATA BREACH NOTIFICATIONS AND LOSS OF PERSONAL INFORMATION 39, 40 (2016).

242. *Id.* at x–xiii.

243. *Id.* at 16.

244. *Id.*

245. *See* Ionut Arghire, *Proposed Law Classifies Ransomware Infection as a Data Breach*, SEC. WEEK (Jan. 22, 2019), https://www.securityweek.com/proposed-law-classifies-ransomware-infection-data-breach.

246. *Id.*

247. *See generally* Justin Hurwitz, *Data Security and the FTC's Uncommon Law*, 101 IOWA L. REV. 955 (2016), (contending that the FTC's facilitation of a common law for data security is ineffective to meet modern security needs); Solove & Hartzog, *supra* note 87 (contending that the FTC's privacy jurisprudence can be expanded to become more effective).

248. *See* Complaint for Permanent Injunction & Other Equitable Relief at 5, Fed. Trade Comm'n v. Rennert, No. CV-S-00-0861-JBR (D. Nev. July 12, 2000).

Rennert, for example, the FTC argued that Rennert had failed to implement an SSL secure connection, a form of standard encryption for communications in transit.[249]

In *TJX Companies*, involving a breach in which hackers gained access to consumers' plain-text payment card information, the FTC argued that it was expected of TJX to implement encryption of sensitive data at rest.[250] In the complaint, the FTC alleged that TJX "created an unnecessary risk to personal information by storing it on, and transmitting it between and within, in-store and corporate networks in clear text."[251] In other words, in both *Rennert* and *TJX*, as well as many other FTC data security complaints, companies are expected to use certain tools to prevent confidentiality compromises.[252]

The same logic should apply to availability. The FTC could use its Section 5 authority to go after companies that do not use reasonable data security practices pertaining to availability, thus threatening the uninterrupted access to critical services and data.

The market may also offer some availability-related solutions that reflect what *reasonable* data security practices mean today. For example, the information security industry offers DDoS mitigation tools that are "designed to combat these attacks by absorbing or deflecting DDoS traffic."[253] In addition, the U.S. Computer Emergency Readiness Team claims that "[w]hile there is no way to completely avoid becoming a target of a DoS or DDoS attack,"[254] companies should still "[e]nroll in DoS protection service[s]."[255] In addition, the National Institute of Standards and Technology offers some helpful and detailed standards for information security, including standards for protecting against availability threats.[256] While voluntary, these

---

249. *Id.*

250. *See* Complaint at 2, *In re* TJX Companies, Inc., No. C-4227 (Fed. Trade Comm'n, July 29, 2008).

251. *Id.*

252. *See id.*; Complaint for Permanent Injunction & Other Equitable Relief, *supra* note 248, at 5.

253. Norton Rose Fulbright, *Legal Implications of DDoS Attacks on the Internet of Things (IoT)*, DATA PROT. REP.: BLOG NETWORK (Dec. 5, 2016), https://www.dataprotectionreport.com/2016/12/legal-implications-of-ddos-attacks-and-the-internet-of-things-iot.

254. U.S. Comput. Emergency Readiness Team, *Security Tip (ST04-015): Understanding Denial-of-Service Attacks*, CYBERSECURITY & INFRASTRUCTURE SEC. AGENCY, https://www.us-cert.gov/ncas/tips/ST04-015 (last updated Nov. 20, 2019).

255. *Id.*

256. *See generally* NAT'L INST. STANDARDS & TECH., FRAMEWORK FOR IMPROVING CRITICAL INFRASTRUCTURE CYBERSECURITY (2018).

standards may still be helpful in guiding enforcement activity in this space.

These tools should reflect the ever-changing standard of reasonable data security practices, which in turn gives legitimacy to the FTC and state authorities under their respective data security statutes in pursuing enforcement actions against entities that are not implementing availability-related defenses.

FTC enforcement may also be directed against IoT manufacturers who produce inadequately secure devices. Indeed, there is evidence that the FTC has already begun to enforce Section 5 of the FTCA against manufacturers that sell unsecure devices.[257] In 2017, the FTC filed a complaint against D-Link, a manufacturer of routers, Internet-protocol ("IP") cameras, and related software and services.[258] In the complaint, the FTC alleged that D-Link misrepresented the level of security of its devices.[259] Similar action against IoT manufacturers, provided they do not implement reasonable data security practices, is likely in the future.

Enforcement is also important for protecting infrastructure. Eighty-five percent of U.S. critical infrastructure is owned by private entities, meaning that many of them are operating under the logic of private profit-driven corporations, where cybersecurity will often be considered as part of a typical cost-benefit analysis.[260] This narrow cost-benefit determination often misses the externalities that society at large may experience, particularly in the context of availability attacks.

D. Statutory Availability

Specific statutes addressing the actors, technologies, and risk factors that amplify and incentivize availability attackers would eventually be needed. For example, as IoT proliferates and makes it easier for availability attacks to take place, legislation focused on it would seem reasonable. Indeed, such a bill had already been introduced in Congress,[261] which would mandate vendors to commit

---

257. *See generally* Complaint for Permanent Injunction & Other Equitable Relief, Fed. Trade Comm'n v. D-Link Corp., No. 3:17-cv-00039 (N.D. Cal. Jan. 5, 2017).

258. *Id.* at 2.

259. *Id.* at 11.

260. *See* Chung, *supra* note 196, at 449.

261. *See generally* Internet of Things Cybersecurity Improvement Act of 2019, S. 734, 116th Cong. (2019).

to patching their products, eliminating vulnerabilities, and relying on standard protocols.[262]

Additionally, focusing legislation on an even narrower subset of technologies may be desirable. For example, vehicles are becoming increasingly dependent on computers, software, data, and networks.[263] Vehicle software today may depend on hundreds of millions of lines of code.[264] With vehicles' default internet connectivity, it would make sense to regulate vehicles' cybersecurity directly. Congress attempted to address the issue of vehicle cybersecurity through a proposed bill,[265] which would have authorized the National Highway Traffic Safety Administration and the FTC to regulate automotive cybersecurity. The bill required critical software systems to be isolated from noncritical systems and vehicles to be equipped with built-in systems to detect and mitigate security breaches.[266] Considering that autonomous vehicles may further distance the user from controlling a vehicle physically, such regulation may appear critical.[267] However, such a bill is yet to pass.[268]

Further congressional attempts to enact new cybersecurity legislation should therefore focus collectively on the actors, risks, threats, and tools surrounding availability attacks. Such legislation should provide incentives to improve cybersecurity in the context of availability as well as deter potential wrongdoing associated with the availability of computers, systems, networks, and data.

---

262. MARK WARNER ET AL., INTERNET OF THINGS: CYBERSECURITY IMPROVEMENT ACT OF 2017 (n.d.).

263. *See* Fredrick Kunkle, *Auto Industry Says Cybersecurity Is a Significant Concern as Cars Become More Automated*, WASHINGTON POST (Apr. 30, 2019, 4:13 PM), https://www.washingtonpost.com/transportation/2019/04/30/auto-industry-says-cybersecurity-is-significant-concern-cars-become-more-automated.

264. David Zax, *Many Cars Have a Hundred Million Lines of Code*, MIT TECH. REV. (Dec. 3, 2012), https://www.technologyreview.com/s/508231/many-cars-have-a-hundred-million-lines-of-code.

265. *See generally* Security and Privacy in Your Car Act of 2017, S. 680, 115th Cong. (2017).

266. *Id.* § 30129.

267. *See, e.g.*, Benjamin L. Bollinger, *The Security and Privacy in Your Car Act: Will It Actually Protect You?*, 18 N.C. J.L. & TECH 214, 242–43 (2017) (arguing that self-driving vehicles require more government regulation in the future).

268. *See* Kristen Hall-Geisler, *Senators Reintroduce a Bill to Improve Cybersecurity in Cars*, TECHCRUNCH (Mar. 23, 2017, 5:18 PM), https://techcrunch.com/2017/03/23/senators-reintroduce-a-bill-to-improve-cybersecurity-in-cars.

E. Security Standards for the Internet of Things

The proliferation of IoT devices creates an increased risk of devastating availability attacks.[269] The market has no incentive to improve IoT security in its current structure. Therefore, mandatory IoT security standards are needed to respond to availability threats. There are some security standards for IoT available, though the law needs to make clear which standards it expects companies to adopt. Some examples include: OWASP,[270] DHS Strategic Principles,[271] One M2M Technical Specification,[272] and more.

The relevant information security authorities, federal and state, need to make clear on which security standards they base their enforcement decisions and provide reasonable notice to covered entities. Congress's attempt to pass the Internet of Things Cybersecurity Act of 2019 is an indication that IoT industry is deficient in robust security standards.[273]

---

269. *See* Kosseff, *supra* note 21, at 999.

270. *See generally IoT Security Guidance*, OPEN WEB APPLICATION SEC. PROJECT, https://www.owasp.org/index.php/IoT_Security_Guidance (last visited Feb. 6, 2021) [https://web.archive.org/web/20200306071714/https://owasp.org/index.php/IoT_Security_Guidance].

271. *See generally* U.S. DEP'T OF HOMELAND SEC., STRATEGIC PRINCIPLES FOR SECURING THE INTERNET OF THINGS (2016) (explaining risks of the rising interconnected nature of devices and suggesting responsible measures to take to avoid future harm).

272. *See generally* ONEM2M, ONEM2M TECHNICAL SPECIFICATION (2014) (defining security solutions for the M2M system).

273. *See generally* Internet of Things Cybersecurity Improvement Act of 2019, S. 734, 116th Cong. (2019).

F. Incentives for Vulnerability Disclosure

Vulnerability disclosure and incentives for security researchers may improve the overall security of computers, networks, and data against availability attacks. If security researchers are free to snoop for vulnerabilities and report them to the relevant actors, the overall number of vulnerabilities will decrease. This is important for the reduction of availability attacks because DDoS attacks are enabled by vulnerable software (which allows the enlisting of vulnerable machines),[274] and ransomware usually takes advantage of a vulnerability in software as well.[275]

Incentivizing ethical hackers to report vulnerabilities to the relevant vendors or authorities could decrease the overall number of exploitable vulnerabilities, narrowing the opportunities for adversaries to mount availability attacks. This could also pressure relevant industries to create secure devices as companies will attempt to avoid public shaming based on flaws in their software detected by security researchers.[276] This will by no means prevent availability attacks entirely; it may, however, decrease their likelihood by increasing the costs associated with mounting an availability attack. This could be achieved through clear distinctions between malicious and benevolent actors and through certain legislative and administrative adjustments, such as clarification of the boundaries of the CFAA and Digital Millennium Copyright Act[277] exemptions in relation to security research.[278]

Recently, different parts of the government have issued calls for security researchers to identify vulnerabilities in exchange for a reward. Hack the Army,[279] Hack the Pentagon,[280] and other initiatives were put in place to provide incentives for security research and

---

274. *See* Chandler, *supra* note 51, at 234 ("DDOS attacks could be reduced by improving software security.").

275. *See id.* at 240.

276. Note, *Immunizing the Internet, or: How I Learned to Stop Worrying and Love the Worm*, 119 HARV. L. REV. 2442, 2450 (2006) ("[M]edia coverage and user complaints can prompt vendors to take action; . . . [otherwise], vendors would be more complacent.").

277. *See generally* 17 U.S.C. § 1201 (2018).

278. *See generally* Kilovaty, *supra* note 99 (arguing for more recognition of the benefits of security research).

279. Christopher Ophardt, *Army Secretary Issues Challenge with 'Hack the Army' Program*, U.S. ARMY (Nov. 21, 2016), https://www.army.mil/article/178473/army_secretary_issues_challenge_with_hack_the_army_program.

280. Press Release, Dep't of Def., Department of Defense Expands 'Hack the Pentagon' Crowdsourced Digital Defense Program (Oct. 24, 2018) (on file with author).

vulnerability disclosure. This could enhance overall information security while warding off future availability attacks.

G. Defining "Unavailability Harm"

Finally, to respond to threat of availability attacks, cybersecurity law will have to define and recognize the harms associated with the unavailability of computers, networks, systems, and data. Currently, data breach litigation largely recognizes financial harms as redressable and actionable,[281] but in light of new information security threats, it is time to include new harms within the scope of existing cybersecurity law frameworks.

Daniel Solove and Danielle Citron argue for the inclusion of risk and anxiety as cognizable harms.[282] According to them, risk and anxiety are just as damaging to a person as financial harms, and therefore litigants should be able to file lawsuits when such harms can be traced to a data breach.[283] Similarly, Jeff Kosseff believes that cybersecurity law is about the *person*, and therefore the law needs to protect victims of online harassment, cyberbullying, cyberstalking, and revenge pornography.[284] Other proposals for new cognizable harms include dignitary harms[285] and manipulation.[286]

The common concern of the aforementioned proposals is that the scope of harm covered by cybersecurity law is too narrow,[287] and new harms reveal the inadequacy of existing law.[288] Availability attacks raise a whole set of new harms that current cybersecurity law does not seek to redress. Is *disruption* a harm? Is the fact that an essential service becomes unavailable due to DDoS a cognizable harm that can serve as the basis for a class action lawsuit? To remain relevant, cybersecurity law will have to recognize the new harms arising out of availability attacks.

V. CONCLUSION

Availability attacks remain an information security challenge for both private and public sector entities. At the heart of this Article is

---

281. *See* Kosseff, *supra* note 221, at 343.
282. *See* Solove & Citron, *supra* note 82, at 756.
283. *See id.* at 737.
284. *See* Kosseff, *supra* note 221, at 350.
285. *See* Ashenmacher, *supra* note 236, at 47.
286. *See* Kilovaty, *supra* note 237, at 456, 470.
287. *See* Kosseff, *supra* note 221, at 343.
288. *See* Ashenmacher, *supra* note 236, at 4.

the gap in cybersecurity law as it pertains to these availability attacks. To alleviate some of the concerns associated with this gap, this Article has proposed seven legal and policy solutions: harmonization of computer crime statutes, disclosure of availability attacks, FTC and state enforcement of reasonable data security practices informed by market-based solutions for availability attacks, the enactment of specific legislation, security standards for IoT, incentives for vulnerability disclosure by security researchers, and defining "unavailability harm." While there is not a single solution to the problem of availability attacks, as this is a polycentric problem, there are nonetheless steps that, if adopted by cybersecurity law, could improve cybersecurity law's ability to deal with the growing threat of availability attacks.