Brooklyn Journal of Corporate, Financial & Commercial Law

Volume 15
Issue 1 *SYMPOSIUM Consumer Structure, Market Structure, and Political Power*

Article 9

12-30-2020

CYBER-INSECURITY: THE REASONABLENESS STANDARD IN INTERNET OF THINGS DEVICE REGULATION AND WHY TECHNICAL STANDARDS ARE BETTER EQUIPPED TO COMBAT CYBERCRIME

Chynna Rose Foucek

CYBER-INSECURITY: THE REASONABLENESS STANDARD IN INTERNET OF THINGS DEVICE REGULATION AND WHY TECHNICAL STANDARDS ARE BETTER EQUIPPED TO COMBAT CYBERCRIME

ABSTRACT

While the Internet of Things (IoT) has created an interconnected world via phones, laptops, and even household devices, it is not infallible. As cyber-attacks increase in frequency, affecting companies of all sizes and industries, IoT device manufacturers have become particularly vulnerable, due in large part to the fact that many companies fail to implement adequate cybersecurity protocols. Mass data breaches occur often. However, these companies are not held accountable due to the use of the reasonableness standard in existing cybersecurity legislation, which is flexible and malleable. In 2019, the California Legislature enacted a cybersecurity law specific to IoT device manufacturers. This Note considers how the existing California IoT legislation fails to hold companies accountable for poor cybersecurity practices through malleable and relaxed standards, and proposes a new standard of industry best practices which looks to a multi-stakeholder initiative to develop more rigorous standards to ensure manufacturers undertake proper cybersecurity initiatives to protect consumer data.

INTRODUCTION

> "Like gods, we have created a new universe called cyberspace that contains great good and ominous evil. We do not know, yet, if this new dimension will produce more monsters than marvels, but it is too late to go back."[1]

References to the Internet of Things (IoT) evoke fantastical images of Heinlein-esque utopias[2] more than they reveal the IoT's true structure—a vast network of connected devices with the capability to communicate with other devices, networks, and the internet.[3] While IoT enthusiasts praise the unparalleled level of interconnectedness and rapid proliferation via new applications such as home security systems, manufacturing, and even "smart

1. David Horsey, *Internet universe contains both marvels and monsters*, BALT. SUN (Aug 4, 2015), https://www.baltimoresun.com/opinion/bal-internet-universe-contains-both-marvels-and-monsters-20150731-story.html.

2. Robert Anson Heinlein (1907–1988) was a famous American science fiction author who often included political themes in his books. *Robert Heinlein Biography*, PEOPLE PILL, https://peoplepill.com/people/robert-a-heinlein/ (last accessed September 20, 2020).

3. Most commonly, IoT devices include cell phones and laptops. Anmar Frangoul, *The Internet of Things: Why It Matters*, CNBC (Oct. 23, 2017), https://www.cnbc.com/2017/10/23/the-internet-of-things-why-it-matters.html.

cities,"[4] the Utopian façade quickly melts away; its dystopian nature manifesting itself as cybercrimes run rampant and consumers lose personal data.[5] In 2012, then Director of the Federal Bureau of Investigation Robert Mueller stated, "[t]here are only two types of companies: those that have been hacked and those that will be [,but] [e]ven that is merging into one category: those that have been hacked and will be again."[6] Oftentimes, device manufacturers fail to implement adequate security features, leaving IoT connected devices amenable to hacking.[7] In 2018, the California legislature sought to reign in a lawless IoT through Title 1.81.26 to Part 4 of Division 3 of the Civil Code (the IoT Security Law).[8] Aiming to strengthen the security of IoT devices by placing cybersecurity requirements on manufacturers of IoT devices sold in California,[9] the statute specifies that any device "capable of connecting to the internet" that is sold in the state must have "a reasonable security feature or features" designed to prevent unauthorized access.[10]

The flexible and indefinite standard in the California statute is the latest in a long history of failed federal and state attempts to define and regulate how companies handle cybersecurity practices in both the public and private sector.[11] Part I of this note addresses the history and growth of the IoT, the background of cybersecurity in the United States, and the legal implications of hacked IoT devices. Part II will then introduce the IoT Security Law and will survey the use of reasonableness in tort law. This section will also analyze existing cybersecurity laws and identify the weaknesses inherent in cybersecurity legislation that incorporates reasonableness. Finally, Part III proposes a new standard that replaces the reasonableness requirement with technical standards that apply best practices as a minimum requirement. This section will also propose an additional solution aimed to enforce these technical requirements prior to prosecution by the Attorney General. Specifically, California should create a multi-stakeholder entity comprised of cybersecurity technical professionals, lawyers, and the California executive, similar to that of the Internet Corporation for Assigned Names and Numbers

4. Smart cities use IoT technology for various functions, including automated transportation, control and oversight of energy and water systems and surveillance. Analytics Vidhya Content Team, *10 Real World Applications of Internet of Things (IoT) – Explained in Videos*, ANALYTICS VIDHYA (Aug. 26, 2016), https://www.analyticsvidhya.com/blog/2016/08/10-youtube-videos-explaining-the-real-world-applications-of-internet-of-things-iot/.

5. Larry Karisny, *IoT Is Changing the Cybersecurity Industry*, GOV. TECH. (Jan. 16, 2018), https://www.govtech.com/security/IoT-Is-Changing-the-Cybersecurity-Industry.html.

6. Stacy Cowley, *FBI Director: Cybercrime will eclipse terrorism,* CNN (March 2, 2012), https://money.cnn.com/2012/03/02/technology/fbi_cybersecurity/index.htm.

7. *See* Karisny, *supra* note 5.

8. The Senate Bill No.327 originally proposed the addition of Title 1.81.26 to Part 4 of Division 3 of the Civil Code. Cal. Civ. Code § 1798.91.04 (West 2018)

9. *Id.*

10. Reasonable security features are defined as those "appropriate" to the "nature and function of the device" and the "information it may collect, contain, or transmit." Cal. Civ. Code, § 1798.91.04(a)(1)-(2)).

11. *See infra* text accompanying notes 73-74.

(ICANN); this entity will first define the necessary technical best practices and, subsequently, to ensure compliance with manufacturers' cybersecurity safeguards prior to a device's data breach. This group will review protocols, assess compliance, and provide oversight and guidance as to improvements needed to meet the industry best practices. Implementation of these reforms will incentivize compliance better than simple enforcement of the California law, thus allowing the state legislature to better achieve its goals of minimizing cyberattacks and data theft.

I. THE BASICS: THE IOT AND CYBERSECURITY

The IoT is "a giant network of connected things and people,"[12] comprising a myriad of connections between devices and the Internet.[13] IoT devices are built with various components that enable connections to the Internet and allow for the transfer and collection of information.[14] IoT platforms facilitate the connections among devices via data networks, allowing for the transmission and aggregation of data from device-users.[15] The IoT devices use Internet transfer protocols to transmit information.[16]

The allure of the IoT is in a large part due to the availability of data. Data and information "is meticulously collected, stored, sold, manipulated, repurposed[,] and reused" from IoT devices.[17] Private companies use the information to understand individuals' preferences, habits, and hobbies.[18] Furthermore, IoT devices aggregate data via "sensor fusion,"[19] allowing for data analysis of multiple devices and ultimately, a better understanding of trends, people, and communities.[20] Aggregated data is critical to companies that collect, analyze, and use information for enhanced and pointed

12. Jen Clark, *What is the Internet of Things?*, IBM (Nov. 17, 2016), https://www.ibm.com/blogs/internet-of-things/what-is-the-iot/.

13. *Id.*

14. Ido Kilovaty, *Freedom to Hack*, 80 OHIO ST. L.J. 455, 466 (2019). Devices such as laptop computers, smartphones, and even self-driving cars are built with software and sensors that enable these devices to connect to an IoT platform. IoT sensors allow for the collection of data "about [the IoT device's] users and environment," while the computer processing unit, commonly referred to as a cloud, processes the collected data. *Id.* The third component of an IoT device, the actuator, executes the actions commanded by the sensor and the cloud. *Id.*

15. *IoT 101: What is an Internet Platform?*, KAA, https://www.kaaproject.org/what-is-iot-platform (last visited Oct. 9, 2019).

16. Andrew Meola, *What is the Internet of Things?*, BUS. INSIDER (May 10, 2018, 1:06 PM), https://www.businessinsider.com/internet-of-things-definition.

17. Janine Hiller & Jordan Blanke, *Smart Cities, Big Data, and the Resilience of* Privacy, 68 HASTINGS L.J. 309, 316 (2017).

18. *Id.*

19. Sensor fusion "dictates that the information from two disconnected sensing devices can, when combined, create greater information than that of either device in isolation." Scott Peppet, *Regulating the Internet of Things: First Steps Towards Managing Discrimination, Privacy, Security and Consent*, 93 TEX. L. REV. 85, 93 (2014).

20. Hiller & Blanke, *supra* note 17, at 316.

marketing.[21] It is not uncommon for IoT device users to become subject to "aggressive advertising . . . surveillance capabilities[,]"[22] or find that their data has been sold to third parties.[23] It is hardly surprising that the sensors used to collect this information are referred to as "ubiquitous,"[24] omnipresent forces that are constantly working to collect information.[25]

The interoperability among IoT devices and the ability to provide consumers with connectivity, convenience, and customization resulted in its rapid worldwide proliferation.[26] With each passing second, an additional 127 devices are connected to the Internet.[27] It is predicted that in 2020, there will be as much as 73 billion IoT connected devices.[28] Sources even estimate that by 2025, there will be more than 125 billion IoT devices worldwide.[29] While some of the explosive growth can be attributed to increases in cellular phone usage and cellular device availability,[30] a portion of this growth has resulted from the expansion of the IoT into new economic markets and industries. IoT markets fall into the following categories: industrial, retail, smart utilities & energy, healthcare, "smart cities," connected homes, wearables, connected cars, and personal health.[31] IoT devices have expanded further into the consumer market as connections to the internet have imparted new functionalities on cars, home appliances, cameras, and even Apple Watches.[32] For instance, by connecting a car to the internet, drivers may soon become obsolete as autonomous vehicles relegate car owners to that of passenger.[33]

---

21. *Id.*

22. Kilovaty, *supra* note 14, at 470.

23. *Id*.

24. *Id*. at 471.

25. *Id*. at 472.

26. Devices can easily be modified and customized to achieve an individual user's desired look or function, and vendors use IoT devices to monitor and assess their products in the hope of increasing revenue. The connections among devices via the IoT platform enable enhanced communication that goes beyond the functionalities of typical online technologies. *Id*. at 470.

27. Kaylie Gyarmathy, *Comprehensive Guide to IoT Statistics You Need to Know in 2020*, VXCHNGE (Mar. 26, 2020), https://www.vxchnge.com/blog/iot-statistics.

28. This is a drastic increase from the 15.41 billion IoT connected devices in 2015, just five years prior. Statista Research Department, *Internet of Things - number of connected devices worldwide 2015-2025*, STATISTA (Nov. 27, 2016), https://www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide/.

29. Gyarmathy, *supra* note 27.

30. *Id.* Some models forecast an approximately 3.5 billion cellular IoT connections by 2023. *Id*.

31. Jane Kirtley & Scott Memmel, *Too Smart for its Own Good: Addressing the Privacy and Security Challenges of the Internet of Things*, 22 NO. 4 J. INTERNET L. 1, 8, 19 (2018).

32. For instance, the market for home IoT devices is expected to grow to 53.45 billion dollars by 2022. Gyarmathy, *supra* note 27. Ronald Hedges & Kevin Ryan, *The IoT: What Is It, What Can Happen With It, And What Can Be Done When Something Happens*, 90-APR N.Y. ST. B.J. 30, 31 (2018).

33. Gyarmathy, *supra* note 27. "Automobiles now have built-in, computer-connected sensors that tell the operator to brake or get back into his or her lane." Hedges and Ryan, *supra* note 32, at 31.

Industry leaders recognize the importance of IoT growth within their own companies.[34] Companies like IBM and Juniper forecast that IoT technology will soon be integrated in 95% of new electronic designs.[35] The staggering amount of resources put into IoT development further support the view that IoT is important for growth.[36] Even the manufacturing industry has expended significant time and resources on implementing IoT devices.[37] Further, investment in the IoT is not limited to only the private sector. A growing number of cities are also investing in "Smart City IoT Technology"[38] for tasks like measuring air pollution, identifying available parking stations, and better connecting citizens to local governments.[39] Cisco, for instance, has defined a "Smart City" as one utilizing "scalable solutions that take advantage of information and communications technology (ITC) to increase efficiencies, reduce costs[,] and enhance quality of life."[40] Companies, like Amazon, invest in smart city technology and market technical solutions to local governments.[41] Crucial to the operation of smart cities is the role of private sector technology companies in contracting with local governments.[42]

A. CYBERSECURITY CONCERNS AND THE IOT

As the IoT becomes ingrained in various facets of our society, it is clear that manufacturers and IoT platform providers do not take appropriate cybersecurity measures to protect information that passes through devices and networks. Data protection is crucial, as "[t]he most private and nonintuitive pieces of information about a user are constantly connected by IoT devices, and may enable misuse."[43] A picture of the IoT is thus

34. Every nine out of ten executives who work in technology claim "IoT growth is critical to their business." Gyarmathy, *supra* note 27.

35. Kirtley and Memmel, *supra* note 31, at 8, 19.

36. Gyarmathy, *supra* note 27.

37. *Id*.

38. *Id*. Domestic cities like New York, Pittsburgh, San Francisco, Louisville, and Columbus all use smart city technologies to innovate transportation, parking, and sustainable energy. *Top 10 Smart Cities in the U.S.*, ROUTE MATCH (Mar. 14, 2017), https://www.routematch.com/top-10-smart-cities-us/.

39. Hiller and Blanke, *supra* note 17, at 311.

40. Hiller and Blanke, *supra* note 17, at 317 (quoting Gordon Falcon and Shane Mitches, *Smart Cities Framework: A Systematic Process for Enabling Smart + Connected Communities*, CISCO, 2 (2012)).

41. Hiller and Blanke, *supra* note 17, at 316–17. The technology giant Amazon is intimately involved with promoting Smart Cities through its Global City Teams Challenge, in which the company provides resources to city teams with the goal of developing and implementing IoT and Smart City Technologies. Amazon even goes as far as to feature its solutions in its Amazon Web Services Marketplace, so cities "can easily understand, test, and adopt technologies that will transform [their] city." *Smart City Solutions From the Global City Teams Challenge*, AMAZON WEB SERVS. MARKETPLACE, https://aws.amazon.com/mp/gctc/ (last visited Oct. 12, 2019).

42. *How can the private and public sectors work together to create smart cities?*, MCKINSEY & CO. (Jan. 2019), https://www.mckinsey.com/industries/capital-projects-and-infrastructure/our-insights/how-can-the-private-and-public-sectors-work-together-to-create-smart-cities.

43. Kilovaty, *supra* note 14, at 472.

incomplete without an understanding of common cyber threats and the importance of cybersecurity in protecting users' data. Unfortunately, cyberbreaches are far too common. In 2017 alone, IoT cyberattacks increased by more than six hundred percent.[44]

The size of a company has little influence on whether or not there will be a cyberattack against it.[45] Since the early 2000's, even billion dollar companies like Yahoo!, Facebook, and Equifax have faced cyberattacks which compromised millions, if not billions, of accounts.[46] The California Attorney General, after analyzing reports on over six hundred breaches occurring between 2012 and 2015, concluded that in "2015 alone, nearly three in five Californians were victims of a data breach."[47] The financial loss to companies is just as staggering a statistic as companies lost two trillion dollars from cybercrimes.[48] In response, there has been an increase on cybersecurity spending in both the private and public sectors.[49]

The ramifications of a cybersecurity breach can have longstanding effects on both a company's financial health and its perception by the public.[50] Financial costs include compensation to customers and declines in share value, leading to lost revenue.[51] Notably, damage to a company's reputation and a loss of trust among customers can reduce future growth and customer base.[52] Additionally, in the event of a data breach, many companies are subjected to "hidden costs" in the form of regulatory fines, lawsuits, and investigations brought by government agencies like the Federal Communications Commission.[53]

---

44. Nick Galov, *Cyber Security Statistics for 2019*, CYBER DEFENSE MEDIA GRP. (Mar. 21, 2019), https://www.cyberdefensemagazine.com/cyber-security-statistics-for-2019/. Additionally, it is estimated that there is a cyberattack once every fourteen seconds, with an average chance of being attacked within the first five minutes of connecting an IoT device. Matt Powell, *11 Eye Opening Cyber Security Statistics for 2019*, CPO MAG. (June 25, 2019), https://www.cpomagazine.com/cyber-security/11-eye-opening-cyber-security-statistics-for-2019/.

45. Shena Tharnis, *As Cyber Attacks Become More Prevalent, Here's Why Your Small Business is at Risk*, SEC. MAG. (Feb. 28, 2020), https://www.securitymagazine.com/articles/91806-as-cyber-attacks-become-more-prevalent-heres-why-your-small-business-is-at-risk#:~:text=In%20fact%2C%20cyberattacks%20on%20small,according%20to%20a%20recent%20report. "In fact, cyberattacks on small businesses are more common than many think, with more than two-thirds (67%) of companies with fewer than 1,000 employees having experienced a cyberattack, and 58 percent having experienced a breach, according to a recent report." *Id.*

46. Powell, *supra* note 44

47. Legis. Bill. Hist. C.A. S.B. 327 (2017).

48. Powell, *supra* note 44. By 2021, this number is expected to reach more than double that amount. Galov, *supra* note 44.

49. The cybersecurity market is expected to reach $300 billion by 2024. Powell, *supra* note 44.

50. Maddie Davis, *4 Damaging After-Effects of a Data Breach*, CYBINT SOLS. (July 25, 2019), https://www.cybintsolutions.com/4-damaging-after-effects-of-a-data-breach/.

51. *Id*.

52. *Id.*

53. *Data Security Breach: 5 Consequences for Your Business*, AME GRP., https://www.theamegroup.com/security-breach/ (last visited Dec. 26, 2019).

The "complexities" of the IoT "magnify cyber risk."[54] Vast connections among devices mean a single device's vulnerability[55] waterfalls down the IoT, infiltrating all connected devices.[56] A single device can infect Wireless Fidelity connections, operating systems, and clouds.,[57] allowing cyberattacks to move upstream and waterfall back down to other devices.

How then, should governments regulate IoT technologies and ensure that companies implement adequate cybersecurity safeguards? One school of thought argues that regulation now could be "premature," "overly rigid," and ultimately, a hindrance to the various IoT markets.[58] Referred to as "permission-less innovation," some scholars assert that the value of IoT to society and the economy warrants minimal regulation, allowing companies to experiment and develop IoT technology as they please.[59] To some extent, a viewpoint that favors minimal regulations is reactionary because future problems should instead be addressed if, *and when*, they occur.[60] The role of the government under the permission-less innovation view is not one of inaction, but instead, promotion.[61] Alternatively, a precautionary approach advocates for harsher regulations on IoT devices to secure information and ensure only necessary data remains on IoT devices for extended periods of time.[62]

II. THE CALIFORNIA IOT DEVICE LEGISLATION AND THE REASONABLENESS IN CYBERSECURITY LAW

The IoT Security Law[63] is the first law to place cybersecurity requirements on IoT manufacturers selling devices within the state. California enacted the legislation due to data privacy and security concerns surrounding the collection of sensitive data by IoT devices, which are often compromised by a cyberattack.[64] The law is designed to protect consumers, who are unaware of the vast amounts of data collected in the IoT and the likely chance of a cyberbreach.[65]

54. Gary Eastwood, *5 of the Biggest Cybersecurity Risks Surrounding IoT Development*, IDG (June 27, 2017, 11:32 AM), https://perma.cc/5D4P-2FC8.

55. Kirtley and Memmel, *supra* note 31, at 19.

56. *Id*. at 20.

57. Nikole Davenport, *Smart Washers May Clean Your Clothes, But Hacks Can Clean Out Your Privacy, and Underdeveloped Regulations Could Leave You Hanging on a Line,* 32 J. MARSHALL J. INFO. TECH. & PRIVACY L. 259, 267 (2016).

58. Adam Thierer, *The Internet of Things and Wearable Technology: Addressing Privacy and Security Concerns Without Derailing Innovation*, 21 RICH. J.L. & TECH 6, 36 (2015).

59. *Id*. at 39.

60. *Id*. at 40.

61. *Id*.

62. *Id*. at 44.

63. Cal. Civ. Code § 1798.91.04-06 (2018).

64. Legis. Bill. Hist. C.A. S.B. 327 (2017).

65. *Id.*

Written to align with California's data breach notification laws,[66] the legislature deemed the IoT Security Law as "common sense," and drafted its provisions to allow for the flexible nature of technology.[67] The IoT Security Law applies to manufacturers of connected devices that are sold or offered for sale in California, as well as entities that contract with a manufacturer to produce products on its behalf.[68] Exemptions also exist for various categories of businesses.[69]

The IoT Security Law's legislative history provides an almost laughable but poignant example of IoT device's security vulnerabilities in "My Friend Cayla" dolls, which are equipped with IoT and Bluetooth technologies.[70] The dolls ask children for personal information like their school names, addresses, and parents' names.[71] The commentary notes that Bluetooth technology is amenable to hacking, which could lead to theft of personal information or the programming of a doll to "utter obscenities or even speak directly to children through the doll from up to 50 feet away."[72] The legislature doubted that a toy manufacturer would take adequate cybersecurity safeguards (or incur the extra costs) to protect the tween dolls without adequate government regulations.[73]

Through the IoT Security Law, California regulates IoT device manufacturers with products sold in the state by subjecting them to "reasonable" security features that must be appropriate (1) "to the nature and function of the device", and (2) "to the information it may collect, contain,

66. Cal. Civ. Code § 1798.82 (2018).

67. Legis. Bill. Hist. C.A. S.B. 327 (2017). To address these innovations and their attendant risks, [the] bill sets out requirements concerning the security of such devices . . . [requiring] manufacturers to ensure these devices are equipped with reasonable security features to protect both the device and the information collected. Legis. Bill. Hist. C.A. S.B. 327 (2017).

68. Cal. Civ. Code § 1798.91.04 (2018).

69. Exemptions include "unaffiliated third-party software or applications that a user chooses to add to a connected device; providers of an electronic store, gateway, marketplace or other means of purchasing or downloading software or applications and entities or individuals subject to HIPAA or the Confidentiality of Medical Information Act with respect to any activity regulated by those acts." Cal. Civ. Code, § 1798.91.06 (2018); *see also* Sharon Klein, *et al.*, *California Becomes First State to Regulate IoT Devices*, TROUTMAN PEPPER (Oct. 3, 2018), https://www.troutman.com/insights/california-becomes-first-state-to-regulate-iot-devices.html.

70. IoT and Bluetooth features in the "My Friend Cayla" dolls allow it to communicate with children using an Internet connection. Legis. Bill. Hist. C.A. S.B. 327 (2017).

71. Legis. Bill. Hist. C.A. S.B. 327 (2017). The idea of high-tech and potentially dangerous IoT dolls is a concept that has also been explored in pop culture, most notably through the 2019 remake of the classic horror movie Child's Play. While the original movie reveals that Chucky has been brought to life through evil spirits, the rebooted Chuckie is" a walking, talking smart device" with "all his safeguards removed by a vengeful factory worker." Richard Jordan, *Child's Play director on upgrading Chucky for the AI era*, DEN GEEK (June 25, 2019), https://www.denofgeek.com/movies/child-s-play-director-on-upgrading-chucky-for-the-ai-era/.

72. Legis. Bill. Hist. C.A. S.B. 327 (2017).

73. *See generally* Theo Douglas, *California Governor Approves Bills Tightening Security, Privacy of IoT Devices*, GOV'T TECH. (Sept. 28, 2018), https://www.govtech.com/applications/Two-Bills-Before-California-Governor-Would-Tighten-Security-Privacy-of-IoT-Devices.html.

or transmit."[74] The legislation specifies that in light of these requirements, IoT devices will meet the "reasonable" qualifications if: "(1) [t]he preprogrammed password is unique to each device manufactured" or "(2) [t]he device contains a security feature that requires a user to generate a new means of authentication before access is granted to the device for the first time."[75]

Use of the term "reasonable security features" in the IoT Security Law, and the subsequent examples for satisfying the requirements, introduce questions related to the effectiveness of the law in preventing cyberbreaches and protecting consumers' personal data. It remains unclear whether incorporation of the term "reasonable" to the statute will strengthen the security of IoT devices to achieve the law's objectives. By abstractly defining "reasonable security features," the legislature failed to account for the various industries and applications of IoT devices, thus failing to provide clear guidance to help companies comply. An abstract definition leaves everyone involved in the IoT infrastructure subject to the California Executive's interpretation of the words, however, neither the Attorney General nor the State has issued guidance as to how the law will be interpreted.[76]

A. UNDERSTANDING REASONABLENESS

A brief background on the use of "reasonableness" in the general practice of law is necessary for insight as to the effectiveness of the term in the IoT Security Law. Often referred to as a "rule of reason,"[77] the standard of reasonableness provides a means for the "application of community standards" in various contexts.[78] Courts use reasonableness to determine legal standards that reflect commonalities among industries, as well as what is "good" by constructing and asking what a reasonable person or company might do."[79] In some ways, the notion of reasonableness involves "thinking about both what people *actually* do and what people *should* do."[80]

The reasonableness standard is perhaps best known in tort law. Specifically, the tort of negligence incorporates the standard by asking whether a defendant took reasonable care.[81] Two different approaches to

74. Cal. Civ. Code § 1798.91.04(a)) (2018). Systems must also be "[d]esigned to protect the device and any information contained therein from unauthorized access, destruction, use, modification, or disclosure." *Id.*

75. Cal. Civ. Code § 1798.91.04(b)) (2018).

76. Jason Tashea, *California imposes new regulations on "internet of things devices,"* A.B.A. J. (Dec. 10, 2018), www.abajournal.com/news/article/new_california_imposes_regulations_on_the_internet_of_things.

77. David Zaring, *Rule by Reasonableness*, 63 ADMIN. L. REV. 525, 525 (2011).

78. *Id.* at 527.

79. Kevin Tobia, *Legal Standards Invoke the "Reasonable Person." Who is it?*, AEON (Jan. 25, 2019), https://aeon.co/ideas/legal-standards-invoke-the-reasonable-person-who-is-it.

80. *Id*.

81. Kevin Tobia, *How People Judge What is Reasonable*, 70 ALA. L. REV. 293, 298–300 (2018).

interpretation of the reasonable standards exist: some assess reasonableness by what is common (the statistical approach),[82] while others focus on reasonableness as what is good (the prescriptive approach).[83] The statistical approach takes a more rigid and mathematical approach, while a prescriptive approach looks to balance the benefits and detriments to those within a group. Neither approach is rooted in expertise within a specific industry or field, but instead are focused on the average perspective. Thus, a reasonable or acceptable practice is not a reflection of best practices, but rather a general consensus.

B. CYBERSECURITY REGULATION USING REASONABLENESS

While the IoT Security Law is unique in that it focuses on manufacturers, the law resembles existing cybersecurity legislation that also incorporates standards of reasonableness. Governments at both the federal and state levels have enacted cybersecurity legislation to regulate private entities that handle sensitive information like personal health information and financial data. Weaknesses present in the Health Insurance Portability and Accountability Act of 1996 (HIPAA)[84] and cybersecurity regulations promulgated by the New York Department of Financial Services (NYFDS)[85] reflect the need for regulations that incorporate stricter security standards beyond mere reasonability.

1. HIPAA

HIPAA resulted from Congress' desire to decrease healthcare costs by minimizing fraud and abuse within the healthcare industry.[86] Medical records, for instance, are purported to be valued on the black market at more than ten times that of the going rate for other personal information like credit

82. The statistical approach "focuses on defining the appropriate standard of precautions to be taken" by looking at how people typically act in a similar situation. It considers what a hypothetical average person might do as a standard for what constitutes the requisite level of care. It does not take into account the expertise or perspective of judges in setting the standard. *Id.* at 299, 301.

83. The prescriptive approach incorporates multiple theories, such as a cost benefit analysis related to welfare maximization, and community values. *Id.* at 302.

84. The Health Insurance Portability and Accountability Act of 1996, 45 C.F.R. §§ 164.502(b), 164.514(d) (2017) [hereinafter HIPAA].

85. Compilation of Codes, Rules, and Regulations of the State of New York Currentness, 23 NY ADC 500.0 (2017) [hereinafter NYCRR 500].

86. HIPAA's associated House Report chronicles the Federal Government's attempts to "improve portability and continuity of health insurance coverage in the group and individual markets, to combat waste, fraud, and abuse in health insurance and health care delivery, to promote the use of medical savings accounts, to improve access to long-term care services and coverage, to simplify the administration of health insurance, and for other purposes," H.R. Rep. No. 104-496, at 69–70 (1996), reprinted in 1996 U.S.C.C.A.N 1865 at 1869. *See also* Deborah Buckman, *Validity, Construction, and Application of Health Insurance Portability and Accountability Act of 1996 (HIPAA) and Regulations Promulgated Thereunder*, 194 A.L.R. FED. 133, 134 (2004).

cards.[87] Medical records contain sensitive information, known as personally identifiable information (PII), and HIPAA guidelines seek to protect this information by placing security requirements on health care providers, plans, and third parties, such as billing companies.[88]

Unlike the IoT Security Law, HIPAA does not regulate manufacturers. Title II, Section F of HIPAA lays out the purpose of the law, which includes "standards and requirements for the electronic transmission of certain healthcare information."[89] Companies covered under HIPAA are required to perform a risk analysis and management in order to determine if security requirements are *reasonable* and appropriate.[90] Reasonable steps include evaluating "the likelihood and impact of potential risks to [electronic personal health information]," [91] "implementing appropriate security measures to address the risks identified in the risk analysis," [92] and "documenting the chosen security measures and . . . the rationale for adopting those measures."[93] Companies must also maintain "continuous, reasonable, and appropriate security protections."[94]

Reasonableness requirements recognize that different entities face unique cybersecurity risks.[95] "What is appropriate [or reasonable] for a particular covered entity will depend on the nature of the covered entity's business, as well as the covered entity's size and resources."[96] If a cyber breach occurs, entities under HIPAA "must take reasonable steps to cure the breach or end the violation."[97] The reasonable and appropriate aspects of the security rule are flexible in that they can be manipulated as long as the "objectives of the requirement" are achieved.[98] Some software companies

87. Caroline Humer & Jim Finkle, *Your Medical Record is Worth More to Hackers than Your Credit Card*, REUTERS (Sept. 24, 2014), https://www.reuters.com/article/us-cybersecurity-hospitals/your-medical-record-is-worth-more-to-hackers-than-your-credit-card-idUSKCN0HJ21I20140924.

88. Glyn Cashwell*, Cyber-Vulnerabilities & Public Health Emergency Response*, 21 J. HEALTH CARE L. & POL'Y 29, 38 (2018).

89. HIPAA § 261. The efforts devoted to developing HIPPA standards with an electronic focus highlight not only the rising prevalence of technology in the healthcare industry at the time, but the potential for increased fraud and abuse within the healthcare industry stemming from the availability of medical records in an electronic format.

90. Cashwell, *supra* note 88, at 38.

91. HIPAA § 164.306(b)(iv).

92. HIPAA § 164.308(a)(1)(ii)(B).

93. HIPAA § 164.306(d)(3)(ii)(B)(*1*); HIPPA § 164.316(b)(1).

94. HIPAA § 164.306(e).

95. *Summary of the HIPAA Security Rules*, U.S. DEP'T. HEALTH & HUM. SERVS., https://www.hhs.gov/hipaa/for-professionals/security/laws-regulations/index.html (last visited Oct. 26, 2019).

96. *Id.*

97. HIPAA § 164.314(a)(1)(ii).

98. *Breaking Down the HIPAA Security Rule*, ACCOUNTABLE (June 2, 2020), https://www.accountablehq.com/post/breaking-down-the-hipaa-security-rule.

even provide online guidance as to how a company can "bend the security rule 'reasonably' and 'appropriately.'"[99]

The adequacy of the HIPAA security rule is called into question when considering the sheer number of data breaches within the healthcare sector each year. In 2019, for example, reports from the United States Department of Health and Human Services published a list of 418 HIPAA breaches that occurred from email breaches and server hacking that led to the compromise of personal data belonging to over 34 million Americans.[100]

The Office of Civil Rights (OCR) is responsible for enforcing HIPAA compliance and investigating companies who violate the law.[101] However, "[t]he vast majority of cases investigated by OCR arise from complaints received rather than from OCR's own fact-finding investigations."[102] If a violation is confirmed, rather than issue fines or impose sanctions on entities who fall under HIPAA, "OCR takes an active role in working with the entities investigated to reform practices that do not comply with HIPAA regulations."[103] In 2014, for example, only seven percent of all cases investigated resulted in a corrective action. Further, there have been 73,288 instances total in which OCR did not take action and investigate potential HIPAA violations.[104] In these instances, OCR independently determined it could not take action because it "did not have the jurisdiction to investigate the entity subjected to the complaint or the perceived privacy violation was simply not covered under HIPAA."[105] This included complaints that were not filed within the requisite time period.[106]

Despite HIPAA's security requirements, numerous breaches and investigations endure, and in some instances, institutions previously investigated by OCR continue to violate the law; in 2019, the University of Rochester Medical Center paid a multi-million dollar fine for failure to encrypt its mobile devices like flash drives and laptops, which led to disclosure of protected data years after a previous investigation for a similar

99. *See HIPAA: How to bend the security rule 'reasonably' and 'appropriately,'* CALYPTIX (Nov. 17, 2014), https://www.calyptix.com/regulations/hipaa-how-to-bend-the-security-rule-reasonably-and-appropriately/.

100. Hoala Greevy, *HIPAA breaches in 2019: A year in review*, PHYSICIANS PRAC. (Mar. 11, 2020), https://www.physicianspractice.com/view/hipaa-breaches-2019-year-review.

101. *See generally Enforcement Process,* U.S. DEP'T HEALTH & HUM. SERVS. (June 17, 2017), https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/enforcement-process/index.html.

102. *The Ultimate HIPAA Guide: The Facts You Need to Know,* EVISIT, https://evisit.com/resources/hipaa-guide/#7 (last accessed Oct. 5, 2020).

103. In more than 24,047 cases, OCR resolved the matters by identifying and assisting entities or companies with implementing corrective practices to ensure that they do not repeat the same violations. *Id.*

104. *Id.*

105. *Id.*

106. *Id.*

issue. [107] Thus, HIPAA's reasonability-focused compliance standard fails to protect peoples' medical records.

2. The New York State Department of Financial Services (NYDFS)

The New York state legislature in turn has focused on reasonability in its efforts to regulate the security practices of private financial institutions. NYDFS's Cybersecurity Regulation,[108] for example, places cybersecurity requirements on certain financial institutions[109] operating within the state,[110] and incorporates reasonable notification requirements in the event of a cyber breach.[111] The NYDFS commented on the reporting requirements, defining a "reasonable likelihood of material [harm]" [112] to include "unsuccessful attacks that appear particularly significant based on the Covered Entity's understanding of the risks it faces."[113] Unlike HIPAA, the NYDFS remains overall, deferential to private financial services, trusting that "Covered Entities will exercise appropriate judgment as to which unsuccessful attacks must be reported and does not intend to penalize Covered Entities for the exercise of honest, good faith judgment."[114] What constitutes a reasonable notification, then, is left to a financial institution's own judgement. As a result, the NYDFS Cybersecurity Regulation not only substitutes government

107. "In 2010, OCR investigated URMC concerning a similar breach involving a lost unencrypted flash drive and provided technical assistance to URMC. Despite the previous OCR investigation, and URMC's own identification of a lack of encryption as a high risk to ePHI, URMC permitted the continued use of unencrypted mobile devices." *Research Center's Failure to Encrypt Mobile Devices Leads to $3 Million HIPAA Settlement*, SEC. MAG. (Nov. 7, 2019), https://www.securitymagazine.com/articles/91236-failure-to-encrypt-mobile-devices-leads-to-3-million-hipaa-settlement.

108. 23 NYCRR 500.

109. These financial institutions are referred to as "Covered Entities" under the legislation. *See generally* 23 NYCRR 500.

110. Juliana De Groot, *What is the NYDFS Cybersecurity Regulation? A Cybersecurity Compliance Requirement for Financial Institutions*, DIGIT. GUARDIAN DATA INSIDER (Oct. 24, 2019), https://digitalguardian.com/blog/what-nydfs-cybersecurity-regulation-new-cybersecurity-compliance-requirement-financial.

111. *Id*. Specifically, "[e]ach Covered Entity shall notify the superintendent as promptly as possible but in no event later than 72 hours from a determination that a Cybersecurity Event has occurred that is either of the following: . . . (2) Cybersecurity Events that have a reasonable likelihood of materially harming any material part of the normal operation(s) of the Covered Entity." 23 NYCRR 500.17(a)(2).

112. 23 NYCRR 500.17(a)(2).

113. "The [NYDFS'] notice requirement is intended to facilitate information sharing about serious events that threaten an institution's integrity and that may be relevant to the [NYDFS'] overall supervision of the financial services industries," and thus may extend beyond solely the effect of causing "material consumer harm.'" *FAQs: 23 NYCRR Part 500 – Cybersecurity*, N.Y. STATE DEP'T. FIN. SERVS., https://www.dfs.ny.gov/industry_guidance/cyber_faqs (last visited Oct. 26, 2019).

114. *Id*.

oversight for private company discretion, but at no point "purport[s] to judge a cybersecurity program's quality"[115]

Further, since enacting the legislation in 2017, the State of New York has hesitated to enforce the law and did not file its first set of charges until July 2020, approximately two years after the breach in that case.[116] Here, First American Title Insurance Company experienced a breach resulting from a cyber vulnerability, which led the NYDFS to accuse the company of violating six provisions of the regulations.[117] However, there are significant issues with the charges because they do not reference particular aspects of the regulations that were not met, but instead argue that the company's cybersecurity program was inadequate.[118] What purpose, then, does this regulation serve if it provides no guidance as to how a company should structure its cybersecurity program or the minimum requisite features that must be met to avoid penalty?

C. COURT EVALUATIONS OF THE REASONABLENESS STANDARD

A vague characterization of the term "reasonable" by both federal and state legislatures is paralleled in the approach taken by courts and agencies. Experts argue that although both technical and legal professionals understand that reasonable cybersecurity features are required, there is no adequate definition of what is "reasonable."[119] As a starting point, some claim that "reasonableness is defined by your company itself. You have to start the process with a risk assessment . . . you have to prioritize, [and] you have to develop a plan. Then you implement appropriate policies, procedures, tools, [and] strategies."[120] Some legal experts have commented that defining the reasonable standard is an exhaustive task that can best be done by summarizing what a reasonable cybersecurity feature *is not*.[121]

Rather than provide a precise definition of the reasonableness standard in the context of cybersecurity, some courts established tests to determine

115. Peter Jaffe, *Problems with New York's first enforcement action under its financial cyber regulations*, FRESHFIELDS BRUCKHAUS DERINGER (July 24, 2020), https://digital.freshfields.com/post/102gc63/problems-with-new-yorks-first-enforcement-action-under-its-financial-cyber-regul.

116. Chris Brook, *NYDFS Charges First Company for Violating its Cybersecurity Regulation*, DIGIT. GUARDIAN (July 30, 2020), https://digitalguardian.com/blog/nydfs-charges-first-company-violating-its-cybersecurity-regulation.

117. *Id.*

118. *See* Jaffe, supra note 115.

119. Bruce Sussman, *Cyberlaw 2019: How Courts See 'Reasonable Cybersecurity'*, SECUREWORLD (Mar. 26, 2019), https://www.secureworldexpo.com/industry-news/reasonable-cybersecurity-2019.

120. *Id.* Data privacy attorney Shawn Tuma has even likened a demonstration of reasonable security to an elementary math class, in that it is up to companies to themselves show the process they go through to implement cybersecurity features. *Id.*

121. Rick Lazio & Mike Davis, *Cybersecurity Risk: What does a 'reasonable' posture entail and who says so?*, CIO DIVE (July 22, 2019), https://www.ciodive.com/news/cybersecurity-risk-what-does-a-reasonable-posture-entail-and-who-says-so/559207/.

whether a company undertook reasonable cybersecurity efforts in the course of its business and in protecting customer data. Of special note is the commonly used "risk/utility" test[122]—a balancing test that asks if the benefits of implementing cybersecurity features outweigh the burdens and costs of putting those features into place prior to a cyberattack.[123] In *In re Adobe Sys. Privacy Litig.*,[124] the U.S. District Court for the Northern District of California, San Jose division, ruled that plaintiff customers of Adobe had standing to assert claims that the company did not maintain reasonable security measures to protect the customers' personal information, since the risk that the customers' personal data would be misused by hackers was immediate and very real, and the customers incurred costs to mitigate the risk of harm.[125] The suit arose out of a July 2013 data breach that occurred when Adobe's servers were hacked, compromising the personal information the company collected from its customers, including names, emails, and credit card numbers.[126] For weeks, the hackers extracted data from servers before third-party security researchers alerted Adobe to the breach.[127] An independent third-party research organization later discovered Adobe source code on the Internet and also alerted Adobe that "researchers [had] concluded that Adobe security practices were deeply flawed and did not conform to industry standards."[128] Adobe's encryption protocol lacked the requisite strength to protect the customer information, and "Adobe similarly failed to employ intrusion detection systems, properly segment its network, or implement user or network level system controls."[129]

The plaintiffs in that case brought a cause of action for violations of parts of the California Civil Code known as the Customer Records Act (CRA).[130] While the court did not specifically rule on whether Adobe's cybersecurity practices were reasonable upon summary judgment, the court did speak to what it considered during a reasonability analysis.[131] The court identified that there was an immediate and real risk that the plaintiffs' personal data would be misused by hackers in the event of a breach."[132]

122. The risk/utility test looks to see "whether a defendant's conduct was reasonable and conformed to others similarly situated in the same industry and if the potential harm outweighs the burden of implementing the proper measures to prevent such harm." *Id*.

123. *See generally* Lazio and Davis, *supra* note 121.

124. *In re Adobe Sys. Privacy Litig.*, 66 F. Supp. 3d 1197 (N.D. Cal. 2014).

125. *Id.* at 1217.

126. *Id.* at 1206.

127. *Id.*

128. *Id.* at 1207.

129. *Id.*

130. The statute stated the following: "A business that owns, licenses, or maintains personal information about a California resident shall implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use, modification, or disclosure." *Id.* at 1210. Cal. Civ. Code §§ 1798.81.5 and 1798.82. (2020).

131. *See supra* note 122 and accompanying text.

132. *In re Adobe Sys. Privacy Litig.*, 66 F. Supp. 3d at 1214.

Similar to legislatures, the Federal Trade Commission (FTC) references "reasonable security" in the agency's IoT device privacy and security guidelines.[133] Under Section 5(a) of the FTC Act,[134] which allows the FTC to sue companies for unfair or deceptive business practices, the FTC has made efforts to hold companies liable for poor cybersecurity practices.[135] In *FTC v. Wyndham Worldwide Corporation*, for example, the FTC brought suit against Wyndham Hotels under the act, citing specific practices that showed the company failed to implement reasonable cybersecurity measures, leading to multiple data breaches and theft of consumers' personal data.[136] The suit resulted in an order for injunction requiring Wyndham to "establish and implement and thereafter maintain a comprehensive information security program . . . that is reasonably designed to protect the security, confidentiality and integrity of cardholder data."[137] However, the Third Circuit also ruled that there is no requirement for the FTC to put companies on notice and publish regulations as to what meets the "reasonable security standards" requirement.[138] While the court mentioned that industry standards can be used to inform companies about what practices are reasonable,[139] it did not account for less straightforward scenarios in which it may be more difficult to make a determination of reasonableness, such as instances a party cannot show that specific cybersecurity practices that are inadequate.

D. IS THE REASONABLENESS STANDARD EFFECTIVE?

As evidenced by the aforementioned healthcare breaches affecting at least 10% of the United States population,[140] and, in 2020, a four hundred percent increase in cyberattacks after the novel coronavirus pandemic,[141] the flexible and malleable nature of the reasonableness standard has neither reduced the chance of cyberattack nor incentivized companies to develop

133. "What constitutes reasonable security for a given device will depend on a number of factors, including the amount and sensitivity of data collected, the sensitivity of the device's functionality, and the costs of remedying the security vulnerabilities." *Internet of Things – Privacy & Security in a Connected World*, FED. TRADE COMM'N 28 (2015), https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf.

134. 15 U.S.C. § 45 (2012).

135. Merritt Baer and Chinmayi Sharma, *What Cybersecurity Standard Will a Judge Use in Equifax Breach Suits*, LAWFARE BLOG (Oct. 20, 2017), https://www.lawfareblog.com/what-cybersecurity-standard-will-judge-use-equifax-breach-suits.

136. F.T.C. v. Wyndham Worldwide Corp., 799 F. Supp. 3d 236, 241 (3d Cir. 2015).

137. Stipulated Order for Injunction at 4 F.T.C. v. Wyndham Worldwide Corp, et al., 10 F.Supp.3d 602 (D.N.J. 2014) (No. 2:13-CV-01887-ES-JAD).

138. F.T.C. v. Wyndham Worldwide Corp., 799 F. Supp. at 255–56.

139. *Id.* at 241.

140. *See generally* Greevy, *supra* note 100.

141. Monstercloud, *Top Cyber Security Experts Report: 4,000 Cyber Attacks a Day Since COVID-19 Pandemic*, CISION PR NEWSWIRE (Aug. 11, 2020 12:45 PM), https://www.prnewswire.com/news-releases/top-cyber-security-experts-report-4-000-cyber-attacks-a-day-since-covid-19-pandemic-301110157.html.

better cybersecurity programs. Incorporating reasonableness so frequently into cybersecurity legislation is retributive rather than proactive because the standard looks back at a company's practices at the time of breach and only reviews a company's cybersecurity safeguards after one has occurred.[142] There is little proof that the reasonableness standard actually reduces security breaches and incentivizes companies to take proper cybersecurity measures prior to the onset of a cyberattack. Though companies bear the responsibility of protecting their systems and devices from a cyberattack, they are not sufficiently incentivized to allot funds to cybersecurity,[143] and as a result companies rely on the ambiguity of the standard to support poor practices.[144]

Respectively, governments are hesitant to regulate cybersecurity standards in the private sector even though more restrictive requirements and stronger cyber defense initiatives are necessary for security.[145] When governments do regulate, they use the confusing reasonableness standard which "offer[s] little specificity as to how to achieve actual compliance."[146] Confusion is exacerbated for companies that operate at multi-national levels because they have the unachievable task of determining what each jurisdiction considers to be reasonable.[147]

The IoT Security Law fails to provide companies with a concrete understanding of what constitutes a reasonable security feature. Like HIPAA, the IoT Security Law does not provide a uniform set of technical requirements or guidance for companies to follow, which allows companies to prioritize savings over adequate cybersecurity. Manufacturers will continue to use the flexible standard to their advantage, manipulating the facts to show that its actions and practices can be construed as reasonable. Further, because manufacturers use reasonableness to skirt the requirements of the law and save money, the industry standard is diluted; the minimal accepted requirements may not be a result of what companies in the industry think is adequate to protect a cyberattack, but instead what is cost effective.

Minimal regulation of private sector companies fosters a mentality in which companies do not prioritize the funding of cybersecurity measures and view these expenses as externalities.[148] Businesses fail to understand the need

142. *See* discussion *supra* Part I.A.

143. James Eastman, *Avoiding Cyber-Pearl Harbor: Evaluating Government Efforts To Encourage Private Sector Critical Infrastructure Cybersecurity Improvements*, 18 COLUM. SCI. & TECH. L. REV. 515, 530 (2017).

144. Cheryl Wang, *Information Privacy and Data Security Laws: An Ineffective Regulatory Framework,* COLUM. UNDERGRADUATE L. REV. BLOG (Oct. 31, 2017), https://blogs.cuit.columbia.edu/culr/2017/10/31/information-privacy-and-data-security-laws-an-inefficient-regulatory-framework/.

145. *See* Eastman, *supra* note 143, at 522.

146. *What are your Legal & Reasonable Obligations when it comes to Cybersecurity?*, HALOCK, https://www.halock.com/what-are-your-legal-obligations-when-it-comes-to-cybersecurity/ (last visited Oct. 26, 2019).

147. *See id*.

148. *See* Eastman, *supra* note 143, at 530.

for adequate cybersecurity measures because "they do not fully internalize the benefits, while others may benefit by being 'free rider[s].'"[149]

III. PROPOSING A NEW STANDARD

Implementing the IoT Security Law with the reasonable language is doomed to fail, as it will neither lessen the risk of breach, nor hold companies accountable for poor cybersecurity practices. Additionally, the unique structure and interconnectedness of IoT devices guarantees that a relaxed standard will only compound the effects of cybercrime, as hackers will be able to infiltrate multiple devices through a single point source. The IoT Security Law must be rewritten to replace the reasonable standard with more technical industry standards and best practices, implementing recommendations promulgated from trade groups like the National Institute for Standards and Technology (NIST), along with findings from the FTC's staff report on the IoT.[150] Implementation of industry guidelines into the statute, however, is no guarantee that companies will comply with the new California law. More must be done to ensure that the statute does not sit idle or is only invoked in the event of a cyberattack. Instead, California's legislature should look to the efforts of non-profit organizations such as ICANN,[151] an organization that handles both coordination of domain names and IP numbers, as well as domain name dispute resolutions, as an example of how to implement technical professionals to provide oversight and guidance to IoT device manufacturers. Further, an established public organization similar to that of ICANN should be created to regulate manufacturers in a proactive way that minimizes both injury from cyberattack and litigation after a cyberattack has occurred.

A. INDUSTRY KNOWLEDGE AND BEST PRACTICES AS A REPLACEMENT FOR THE REASONABLENESS STANDARD

1. Why Best Practices are Beneficial to IoT Regulation – Moving Beyond Industry Standards

Industry standards[152] and best practices are valuable tools because they incorporate norms within a field and address what a particular industry considers adequate. Industry standards are not customizable to an individual

149. *Id.* at 530.

150. Ieuan Jolly, *FTC Recommends Privacy and Security Best Practices for the "Internet of Things*," 20160513A NYCBAR 140, 140 (2015).

151. *See generally* IP2 Business Law Monographs 18.01, Copyright 2019, Matthew Bender & Company, Inc.

152. "As the name implies, an industry standard is the average by which those in a particular field govern themselves. It is the ordinary manner of doing things in that field and can serve to establish different things in various legal settings." *What is the Relevance of "Industry Standards" Under the Law?*, HG LEGAL.ORG LEGAL RESS., https://www.hg.org/legal-articles/what-is-the-relevance-of-industry-standards-under-the-law-36794 (last visited Nov. 22, 2019).

company, but arise from a general consensus as to what is acceptable in daily practice.[153] Further, industry standards prevent courts from viewing a company in a vacuum, and instead gauge performance in relation to what those within the practice are doing and deem acceptable.[154] Accepted industry standards, while not necessarily binding unless present in statute, can potentially provide clarity to courts when assessing liability.[155] The invocation of industry standards often arises in the context of tort and contract litigation.[156] In personal injury litigation, for example, safety standards are used to determine whether a defendant has been negligent.[157] By relying on business practices present within an industry, courts can establish the duty of care that a defendant owes to a plaintiff in preventing an accident.[158] These standards are developed "by consensus,"[159] and enable courts to rule not only consistently, but in a way that recognizes the complexities and differences among industries.

In many ways, the duty of care in preventing an accident is similar to a duty to prevent a cyberbreach or cyberattack. Scholars have proposed a new tort of "negligent enablement"[160] that holds software vendors liable for failure to incorporate reasonable security measures into their products and services.[161] The need for liability in the context of cybersecurity is warranted, given that vendors and manufacturers are better able to protect against cyberbreaches than product users.[162]

However, many judges lack technical competency and are unfamiliar with the topic of cybersecurity, thus making it difficult for courts to accurately assess whether a company has undertaken "reasonable cybersecurity measures" in the manufacture of its IoT devices. Though the America Bar Association has, in its Model Rules of Professional Conduct, incorporated a duty to be competent in technology to "keep abreast of

153. *Id.*

154. *See id.*

155. Thilo Schmidt, *The legal significance of standards*, DIN, https://www.din.de/en/about-standards/standards-and-the-law/legal-significance-of-standards (last visited Nov. 22, 2019).

156. *What is the Relevance of "Industry Standards" Under the Law?*, *supra* note 154.

157. Harry M. Philo, *Use of Safety Standards, Codes and Practices in Tort Litigation*, 41 NOTRE DAME L.REV. 1, 1 (1965).

158. The notion of relying on industry standards is not novel to the courts. Judge Learned Hand famously spoke to courts' reliance on industry best practices to determine negligence. "There are, no doubt, cases where courts seem to make the general practice of the . . . [industry] the standard of proper diligence; we have indeed given some currency to the notion ourselves. . ." *The T.J. Hooper*, 60 F.2d 737, 740 (2d Cir. 1932).

159. Philo, *supra* note 158, at 3–4.

160. Michael L. Rustad & Thomas H. Koenig, *The Tort of Negligent Enablement of Cybercrime*, 20 BERKELEY TECH. L.J. 1153, 1553 (2005).

161. *Id.* at 1557–8.

162. *Id.* at 1558.

changes in law and practice," these rules do not extend to judges.[163] The ABA and many state judicial conduct codes are instead devoid of any duty or requirement to understand technology or cybersecurity.[164] Evaluating whether an IoT manufacturer has built its device with "reasonable" security features requires a level of technological understanding that many judges cannot comprehend without guidance from professionals or experts. Replacing the reasonableness standard in the IoT Security Law with industry best practices will promote consistency and more accurate results, as judges will use these heightened and more technical requirements to guide them in the decision-making process. Courts will thus be required to issue decisions that align with what industry experts have deemed acceptable.

IoT technology industry best practices provide guidance as to what technologists consider adequate cybersecurity measures, given the cost of implementing security features and the prevalence of cyberattacks within the industry. Established industry best practices in the IoT Security Law will safeguard against courts' and governments' inability to understand the nuances of IoT technology.

2. Using Government Led Multi-Stakeholder Initiatives to Create a New Standard of Industry Best Practices

Many critics question the role of government in the regulation of technology, especially when industry curated standards reflect a better understanding of acceptable practices. Self-regulation schemes in the private security and military industries have grown to reflect the development of the industry,[165] as companies issue "codes of conduct" that apply to the entirety of an industry.[166] Enforcement of industry standards within these sectors is successful through voluntary self-compliance,[167] as companies recognize the collective benefit when individual companies adhere to codes of conduct developed by trade associations.[168] Self-regulation within the private security and military industries is not, however, without fault. Some question the efficacy of sanctions and the extent of individual accountability in any private industry.[169] Self-regulation can lead to opportunistic behavior in which actors

163. Robert Ambrogi, *It's Time to Extend the Duty of Tech Competence to Judges*, EVOLVE L. (May 6, 2019), https://abovethelaw.com/legal-innovation-center/2019/05/06/it-is-time-to-extend-the-duty-of-tech-competence-to-judges/?rf=1.

164. *Id*.

165. *See* Daphne Richemond-Barak, *Can Self-Regulation Work? Lessons From the Private Sector and Military Industry,* 35 MICH. J. INT'L L. 773, 779 (2014).

166. *Id.* at 776.

167. *Id*. at 778.

168. Renee De Nevers, *The Effectiveness of Self-Regulation by the Private Security and Military Industry*, 30 J. PUB. POL'Y 119, 220-221 (2010).

169. *See* Richemond-Barak, *supra* note 165, at 792.

who choose not to comply with the industry norms abuse their privileges while remaining undetected.[170]

It is not difficult to envision a scenario in which the IoT device industry, and even the technology industry as a whole, succumbs to opportunistic behavior by individual actors. Self-regulation of privacy has proven itself to be a failure,[171] as a lack of accountability, transparency, and consequences encourage noncompliance.[172] Self-regulation may lead the government to place too much trust in the private sector. As early as the Clinton Administration's 1997 "Framework for Global Electronic Commerce,"[173] the government has been reluctant to regulate technology, and instead has encouraged it to grow unchecked.[174] The Clinton framework referenced government involvement when "needed" and stated that in promoting commerce, its role was to provide support via a "predictable legal environment."[175] "Where governmental involvement is needed," the Framework continued, "its aim should be to support and enforce a predictable, minimalist, consistent, and simple legal environment for commerce."[176] Depending on the policy goals of an administration, government deference to self-regulation can instead lead companies to maximize profits rather than devote a portion of expenditures to cybersecurity.[177] More recently under the Trump Administration, the Department of Transportation advocated for reduced self-regulation in the context of "autonomous vehicle cybersecurity technology."[178]

---

170. *Id.* at 793.

171. Ira S. Rubinstein, *Privacy and Regulatory Innovation: Moving Beyond Voluntary Codes*, 6 ISJLP 355, 356 (2011).

172. *Id.* at 366.

173. President William J. Clinton & Vice President Albert Gore, Jr., *A Framework for Global Electronic Commerce*, WHITE HOUSE (July 1, 1997), https://clintonwhitehouse4.archives.gov/WH/New/Commerce/read.html.

174. The Clinton Administration's position regarding the proliferation of the Internet was that "[g]overnments should encourage industry self-regulation private sector leadership" and "avoid undue restrictions on electronic commerce." "[P]arties should be able to enter into legitimate agreements to buy and sell products and services across the Internet with minimal government involvement or intervention." *A Framework for Global Electronic Commerce Executive Summary*, WHITE HOUSE, https://clintonwhitehouse4.archives.gov/WH/New/Commerce/summary.html (last visited Aug. 23, 2020). Ryan Hagemann, Jennifer Huddleston Skees, & Adam Thierer, *Soft Law for Hard Problems: The Governance of Emerging Technologies in an Uncertain Future*, 17 COLO. TECH. L.J. 37, 85 (2018).

175. Hagemann, Huddleston Skees, & Thierer, *supra* note 174, at 86.

176. President William J. Clinton & Vice President Albert Gore, Jr., *A Framework for Global Electronic Commerce*, WHITE HOUSE (July 1, 1997), https://clintonwhitehouse4.archives.gov/WH/New/Commerce/read.html.

177. The Darkening Storm of Cyberterrorism: International Policy Adaptation for Automotive Cybersecurity Regulations, 59 JURIMETRICS J 267, 289 (2019).

178. Frighteningly, the DOT has championed a mentality that fails to comprehend the long-term implications of inferior cybersecurity protections, and instead looks to encourage "new entrants" to the market. 149 NAT'L HIGHWAY TRAFFIC SAFETY ADMIN., AUTOMATED DRIVING SYSTEMS 2.0, at i, 1 (2017), https://www.nhtsa.gov/sites/nhtsa.dot.gov/files/documents/13069a-ads2.0_090617_v9a_tag.pdf.

A multi-stakeholder initiative can be an effective solution to the issue of poor cybersecurity practices. The Cybersecurity Act of 2015 (the Act) is one example in which collaboration between the private and public sector has resulted in the strengthening of cybersecurity programs.[179] Under the Obama Administration, the Act provided a channel for communication between the government and the private sector that allowed entities to share cybersecurity threat information in a way similar to that shared within the industry.[180] Relying on the framework of a voluntary sharing program, the Act authorizes companies to share information with the Department of Homeland Security.[181] This information is used by the government to develop cybersecurity tools and fight cyberattacks in both the private and public sectors.[182] Extending a multi-regulatory scheme to IoT device regulation is one possible way to remove the ambiguity and ineffectiveness associated with the standard of reasonableness. In reconstructing the IoT Security Law's cybersecurity regulations, the California legislature must incorporate these types of solutions to ensure that the statute encourages IoT device manufacturers to implement appropriate cybersecurity measures. This requires collaboration with existing resources, like NIST's IoT cybersecurity framework, as well as conversations with technologists in the industry. In contrast to the current policy in the United States, international government regulation and active participation in the development of industry standards in has resulted in the creation of "privacy covenants," which represent a fruitful intersection between the government and trade standard regulations.[183] The Dutch Data Protection Authority, for example, reviews privately developed codes to ensure compliance with Dutch statutes,[184] thus striking a balance between industry expertise and government oversight.

At the federal level, the FTC has addressed IoT security via privacy and security best practices and recommendations for the IoT.[185] Focusing on the

See also The Darkening Storm of Cyberterrorism: International Policy Adaptation for Automotive Cybersecurity Regulations, *supra* note 178.

179. Consolidated Appropriations Act, 2016, Pub. L. No. 114-113, 129 Stat. 2242, 2935-85 (codified at 6 U.S.C. §§ 1501-1532 (2017)).

180. What You Need to Know About the Cybersecurity Act of 2015, LATHAM & WATKINS: CLIENT ALERT COMMENT. (Feb. 18, 2016), https://www.lw.com/thoughtLeadership/lw-Cybersecurity-Act-of-2015.

181. *Id.*

182. *Id.*

183. These privacy covenants aim to enforce Dutch data protection laws among industries by inviting the private sector to develop industry codes for processing personal data in relevant respective industries. Rubinstein, *supra* note 172, at 400.

184. *Id.*

185. This seventy-one page staff report, issued by the FTC in 2015, addressed the rise of IoT devices within various industries, in addition to the risks and benefits of the IoT device industry on trade and business practices. Notably, and perhaps problematically, "the report does not discuss devices sold in a business-to-business context . . ." Though not to be addressed in this note, the report's failure to discuss business-to-business interactions could potentially cause concern that while the Federal and California governments' aim of the legislation and reports are to protect

implications of poor IoT device security and the effect on privacy, the FTC staff report detailed the application of traditional privacy principles to the industry.[186] The first portion of the report discusses how existing privacy guidelines from the Fair Information Practice Principles (FIPP) can be applied in the IoT space.[187] Notable is the "Commission Staff's Views and Recommendations for Best Practices,"[188] which articulates the FTC staff's perspective and recommendations for implementing data security features for IoT devices. While the FTC staff expresses the general consensus that there should be reasonable security features,[189] the report goes further and specifies security best practices that companies should consider implementing into daily operations and manufacturing of the IoT devices.[190] Though the report only suggests implementation of these practices, it also warns businesses that the FTC can hold companies to these standards via enforcement actions and existing data privacy legislation.[191]

B. NIST AS A FRAMEWORK AND STANDARD FOR CALIFORNIA IOT DEVICE REGULATION

To adequately address its policy goals and enact an effective statute, California must look to guidance from NIST in the redrafting of its IoT device security guidelines.[192] NIST plays a critical role in the marriage of private sector and government cybersecurity practices through its publications, which detail best practices and recommendations for various science and

consumers, failing to regulate IoT devices in this context may not achieve the intended result of reducing cyberattacks and the associated costs with resulting data breaches. FED. TRADE COMM'N, INTERNET OF THINGS – PRIVACY & SECURITY IN A CONNECTED WORLD 6 (Jan. 2015), https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf.

186. *Id.* at 19–26.

187. FIPPs are a series of five privacy principles that are rooted in the United States Department of Health, Education, and Welfare (HEW) report from 1973. These principles include Notice/ Awareness, Choice/ Consent, Access/ Participation, Integrity/ Security and Enforcement/Redress. Daniel J. Solove and Woodrow Hartzog, *The FTC and the New Common Law of* Privacy, 114 COLUMBIA L. REV. 583, 592 (2014). *See generally Fair Information Practice Principles (FIPPs)*, FED. TRADE COMM'N (March 9, 2010), http://www.ftc.gov/reports/privacy3/fairinfo.shtm.

188. INTERNET OF THINGS, *supra* note 186 at 27–46.

189. *Id.* at 27.

190. The FTC staff report identifies six security best practices that companies should implement in aiming for a "reasonable security" program. These include: (1) security by design, (2) personnel practices, (3) retention of service providers that are also capable of reasonable security practices, (4) a defense-in-depth approach that meets security levels via tools like encryption, (5) reasonable access control monitoring procedures, and (6) security monitoring throughout the entirety of a life cycle. *Id.* at 28-32.

191. Jolly, *supra* note 150, at 140.

192. Founded in 1901, NIST "is responsible for establishing technology, standards, and metrics to be applied to the science and technology industries." Notably, NIST is a multi-dimensional body, as it not only issues recommendations for standards, but is one of the country's oldest science labs and a part of the United States Department of Commerce. Martin Horan, *What is NIST? Understanding Why You Need to Comply*, FTP TODAY (May 22, 2019), https:// www.ftptoday.com/blog/what-is-nist.

technology industries.[193] The standards developed by NIST are derived from conversations among those industry organizations, as well as documents like security publications.[194] Through its best practice guidelines, NIST champions an active dialogue approach.[195] These conversations led the federal government to incorporate NIST's Cybersecurity Framework into its recommendations and policies to strengthen and secure critical infrastructure within the United States,[196] such as town electricity, gas, sewage, and water systems.[197] Those who support NIST assert that each guide "harmonizes industry best practices,"[198] via a "flexible and cost-effective approach to enhancing cybersecurity."[199] As a result, NIST guidelines are valuable and have been used by private and public entities as a means of "assessing and managing cyber risk."[200] Some governments even consider the Cybersecurity Framework mandatory in the context of critical infrastructure.[201]

In May 2020, NIST released a draft of its "Foundational Cybersecurity Activities for IoT Device Manufacturers" guide,[202] which highlights industry best practices for IoT devices and provides a reference point for manufacturers to start implementation of adequate cybersecurity features.[203] The NIST Framework focuses on device and data security, first, by highlighting the vulnerabilities in IoT devices[204] and identifying six core security features for manufacturers to address during device development.[205]

193. Scott J. Shackelford, Scott Russell, and Jeffrey Haut, *Bottoms Up: A Comparison of "Voluntary" Cybersecurity Frameworks*, 16 U.C. DAVIS BUS. L.J 217, 221 (2016).

194. Nate Lord, *What is NIST Compliance?,* DIGITAL GUARDIAN (Oct. 7, 2020), https://digitalguardian.com/blog/what-nist-compliance.

195. *See* Shackelford, Russell & Haut, *supra* note 193, at 222-23.

196. *Id.* at 223.

197. John Verry, *Why the NIST Cybersecurity Framework Isn't Really Voluntary*, PIVOT POINT SEC.: INFOSEC STRATEGIES (last updated May 25, 2017), https://www.pivotpointsecurity.com/blog/nist-cybersecurity-framework/.

198. Shackelford, Russell, & Haut, *supra* note 193, at 222. [Scott Shackelford, Scott Russell and Jeffrey Haut, *Bottoms Up: A Comparison of "Voluntary" Cybersecurity Frameworks*, 16 U.C. DAVIS BUS. L.J 217, 222 (2016).]

199. *Id.*

200. *See id.*

201. Many municipal governments state that if "cybersecurity practices were ever questioned during litigation or a regulatory investigation, the 'standard' for 'due diligence' was now the NIST Cybersecurity Framework." Verry, *supra* note 197.

202. Michael Fagan et al., Foundational Cybersecurity Activities for IoT Device Manufacturers (May 2020) (National Institute of Standards and Technology), NISTIR 8259, https://nvlpubs.nist.gov/nistpubs/ir/2020/NIST.IR.8259.pdf.

203. "The NIST Baseline takes these considerations to the manufacturing side, offering (as NIST describes it) to help IoT device manufacturers 'understand the cybersecurity risks their customers face' so IoT devices can provide the minimal features to make them securable." Steven Augustino, *Securing IoT Devices (Part 2): Inside the NIST Guidance Document for IoT Device Manufacturers,* JD SUPRA (Aug. 24, 2019), https://www.jdsupra.com/legalnews/securing-iot-devices-part-2-inside-the-94616/.

204. *Id.*

205. These core security features include device identification, device configuration, data protection, logical access to interfaces, software and firmware updates, and cybersecurity event logging. *Id.*

NIST recommendations, while not typically binding, can encourage the private sector to adopt appropriate security measures that minimize the threat of attack through strict requirements and public-private sector collaboration.[206] Failing to implement appropriate cybersecurity features can lose a company business, damage its reputation, and affect performance levels within the institution.[207] While NIST compliance can provide an added layer of assurance that a company has implemented adequate cybersecurity measures,[208] it can also provide peace of mind to customers and government agencies by reassuring them that even in the event of a cyberattack, a company has done the best it can to secure its infrastructure and protect data. The notoriety of NIST guidelines among technical professionals and industries makes implementation of standards set forth in the "Core Cybersecurity Feature Baseline for Securable IoT Devices" guidelines particularly appealing. The NIST framework incorporates language that "invokes personal responsibility of users by looking to make basic cybersecurity best practices common knowledge."[209] Thus, these guidelines can provide customers with educational tools necessary to hold companies accountable for their data and cybersecurity practices.[210] Finally, NIST is valuable in that its frameworks provide well-defined and clear technical guidelines that specify what is sufficient to effectively counter a cyberattack. California should implement the NIST framework into the IoT Security Law to create a concrete set of guidelines for industries to follow and allow for consistent enforcement of the statute.

C. BEYOND THE LEGISLATION: ENSURING COMPLIANCE VIA REGULATORY COALITION

Implementation of industry standards and best practices to California's IoT Security Law is only part of the solution to ensure IoT device manufacturers adopt heightened cybersecurity requirements. Per the statute, the Attorney General is responsible for investigating and penalizing IoT manufacturers for failure to adhere to the law,[211] and usually, government entities do not investigate and enforce until after the cyberattack and breach has occurred. Additionally, because case law surrounding the IoT Security

206. *See* Horan, *supra* note 192.

207. *Id.*

208. Lord, *supra* note 194.

209. Jared Magill, *The Crooked Path to Determining Liability in Data Breach Cases*, WIRED https://www.wired.com/insights/2015/03/crooked-path-determining-liability-data-breach-cases/ (last visited Oct. 5, 2020).

210. *See generally id.*

211. John P. Rondini, *The Countdown Begins on California's "Internet of Things" Law*, LEXOLOGY (Oct. 28, 2019), https://www.lexology.com/library/detail.aspx?g=24ba314b-cf82-418b-a6a6-0b3ac7fdbd64.

Law is nonexistent,[212] a company may wait to implement adequate security features until the courts have provided guidance to ensure compliance. In some sense, the unintended consequences of the IoT statute parallels the effects of retributive sentences in criminal law. While "retributive justice," or punishment for one's actions is a valid objective, some argue that it conflicts with other preventive goals, such as minimizing or preventing "antisocial behavior."[213] Through the retributive justice framework, conduct is regulated via punishment after an act occurs, with an underlying assumption that it will "eliminate the occurrence" of a particular wrong.[214] Would a similar model, then, incentivize companies to take the appropriate measures prior to punishment from the Attorney General? It seems doubtful because, as discussed earlier, legislation up until this point has failed to effectively remedy the issue.

To ensure compliance prior to a statutory violation, California must create a regulatory body to evaluate and oversee adherence to industry best practices. ICANN and its role in administration of the internet and disputes[215] can serve as a model for a potential state entity to review and confirm IoT device compliance prior to a cyberbreach or attack. While ICANN primarily shares responsibility in the coordination and maintenance of internet protocol addresses, it also plays a role in policy.[216] ICANN thus ensures the internet runs smoothly and securely among all participants.[217] A similarly created state and non-profit coalition, consisting of technical professionals as well as lawyers, would push IoT device manufacturers to take preventative measures to implement adequate security features and remain cognizant of the IoT Security Law. This coalition will not only utilize its professional expertise to specifically determine the technical standards that comprise industry best practices but will also monitor these companies to ensure the cybersecurity best practices are implemented.

212. Stacy Higginbotham, *Is the world ready for California's new IoT laws?*, STACEY ON IOT (Dec. 2, 2019), https://staceyoniot.com/is-the-world-ready-for-californias-new-iot-laws/.

213. Edward K. Cheng, *Structural Laws and the Puzzle of Regulating Behavior*, 100 NW. U.L. REV. 655, 672–73 (2006). IoT manufacturers may, for example, exhibit antisocial behavior by undertaking poor cybersecurity practices at the expenses of other companies who try to implement adequate measures.

214. Louis Kaplow & Steven Shavell, *Fairness Versus Welfare*, 114 HARV. L. REV 961, 1007 (Feb. 2001).

215. *What does ICANN do?*, ICANN AT-LARGE, https://atlarge.icann.org/about/what-does-icann-do (last visited Dec. 25, 2019).

216. The organization also "facilitates the process of policy development that will enable technical changes to how the unique identifiers are run." *Id.*

217. *See id.*

CONCLUSION

The IoT Security Law went into effect on January 1, 2020, and though the state is the first to hold companies accountable to requisite cybersecurity standards for IoT devices, [218] the law does so by implementing the ill-defined standard of reasonableness. By incorporating the reasonableness standard into the law, the California legislature provides little guidance to the Attorney General and courts as to what constitutes adequate cybersecurity protections. [219] Without stringent security requirements and a better understanding of whether a company is taking the correct steps to implement appropriate security features, there is a real threat that the legislation will be ineffective.[220]

The California legislature must significantly revamp the Internet Security Law to include more rigorous IoT industry standard security requirements, as well as develop a regulatory coalition of technical and legal professionals to ensure compliance prior to breach. By shifting the legislation's retributive approach to one of proactivity via government and private collaboration, a compliance model based on industry standards is better equipped to protect consumer information passing through the IoT network.

Chynna Rose Foucek[*]

218. Jerry Bowles, *SB-327 Passes as California Steps Up With Nation's First IoT Security Bill – Is It Useful?*, DIGINOMICA (Sept. 23, 2018), https://diginomica.com/iot-security-california-sb-327-first.

219. *See id.*

220. Robert Graham, *California's Bad IoT Law*, ERRATA SECURITY (Sept. 10, 2018), https://blog.erratasec.com/2018/09/californias-bad-iot-law.html#.XgY8HEdKg2x.

* B.A., Rice University, 2015; J.D. Candidate, Brooklyn Law School, 2021. Thank you to the Brooklyn Journal of Corporate, Financial & Commercial Law editorial board for their thoughtful feedback and thorough reviews throughout the editing process. And thank you to my family and close friends who listened to me ramble on these last few years about the intersection of cybersecurity, technology and the law - in the hopes of trying to make sense of muddled doctrines and posit meaningful solutions.