Have You Updated Your Toaster? Transatlantic Approaches to Governing the Internet of Everything

SCOTT J. SHACKELFORD† & SCOTT O. BRADNER†

As Internet-connected devices become ubiquitous, it remains an open question whether security—or privacy—can or will scale, or whether a combination of perverse incentives, new problems, and new impacts of old problems like "technical debt" amassing from products being rushed to market before being fully vetted, will derail progress and exacerbate cyber insecurity. This Article investigates contemporary approaches to Internet of Things (IoT) governance through an in-depth comparative case study focusing on the European Union (EU) and the United States. Particular attention is paid to the impact on IoT security of the General Data Protection Regulation (GDPR) and the Network Information Security (NIS) Directive in the EU, and the influence of the U.S. National Institute for Standards and Technology Cybersecurity Framework (NIST CSF), with a focus on mitigating the risk of politically motivated attacks on civilians. We analyze reform proposals and apply lessons from major prior Internet governance debates to argue for a polycentric approach to improving IoT security and privacy in the transatlantic context.

† Chair, IU-Bloomington Cybersecurity Program; Director, Ostrom Workshop Program on Cybersecurity and Internet Governance; Associate Professor, Indiana University Kelley School of Business.

† Harvard University, retired.

TABLE OF CONTENTS

INTRODUCTION 629
I. WELCOME TO THE INTERNET OF EVERYTHING 632
A. HISTORICAL DEVELOPMENT 633
B. TECHNICAL VULNERABILITIES AND USE CASES 633
C. AN IOT MARKET FAILURE? 635
D. CONSIDERING A ROLE FOR INSURANCE 636
E. A POLYCENTRIC APPROACH TO SECURING IOT 637
II. U.S. CASE STUDY 640
A. FEDERAL REGULATORY LANDSCAPE 641
B. ANALYZING THE NIST CSF 644
C. CASE FOR A NIST IOT FRAMEWORK 645
D. UNPACKING THE PROPOSED FEDERAL IOT LEGISLATION 645
E. CIVIL SOCIETY 646
III. E.U. CASE STUDY 647
A. GDPR'S APPLICATION TO IOT SECURITY 648
B. NATIONAL CASE STUDY: UNITED KINGDOM & BREXIT 648
C. SUMMARY 651
IV. POLICY IMPLICATIONS 652
A. POLYCENTRIC INSTITUTIONAL ANALYSIS 653
B. LOOKING BACK: APPLYING LESSONS FROM INTERNET GOVERNANCE TO IOT SECURITY 655
C. LOOKING AHEAD: OPERATIONALIZING CYBERSECURITY DUE DILIGENCE IN THE IOT CONTEXT 657
CONCLUSION 661

INTRODUCTION

There were more than 2.9 billion cyber attacks on Internet of Things (IoT) devices in 2019, which works out to a 300-percent increase from 2018, resulting in damages measured in the billions.[1] Regardless of the specific number, such a vast scale of Internet-connected devices opens up a host of both business possibilities and security vulnerabilities. One such example of a potentially dystopian IoT future came in 2016 when a distributed denial of service (DDoS) attack, which came to be known as the Mirai botnet,[2] crashed servers managed by Dyn, a leading tech firm that manages certain critical Internet services, resulting in service disruptions. The botnet took advantage of IoT vulnerabilities,[3] but instead of a foreign nation state, it turned out that the perpetrators were three college students trying to win at Minecraft.[4] "They didn't realize the power they were unleashing," according to FBI agent Bill Walton.[5] "This was the Manhattan Project."[6]

This episode highlights the myriad vulnerabilities underlying the Internet's architecture that politically motivated nation-states can leverage to achieve their strategic ends, such as undermining trust in an adversary government by causing civil unrest following a blackout.[7] During the 2018 Black Hat cybersecurity conference, for example, ninety-three percent of respondents "saw the future of IoT not necessarily as something smarter, but more dangerous, as they predict nation states will target or exploit connected devices in droves over the coming year."[8]

The advent of Internet-connected vehicles and appliances has the capacity to revolutionize business and society.[9] But the vast majority of IoT devices are

---

1. Zak Doffman, *Cyberattacks on IOT Devices Surge 300% in 2019, 'Measured in Billions', Report Claims*, FORBES (Sept. 14, 2019, 2:42 AM), https://www.forbes.com/sites/zakdoffman/2019/09/14/dangerous-cyberattacks-on-iot-devices-up-300-in-2019-now-rampant-report-claims/#7771c6758926.

2. *See* Neena Kapur, *The Rise of IoT Botnets*, AM. SEC. PROJECT (Jan. 13, 2017), https://www.americansecurityproject.org/the-rise-of-iot-botnets/ ("A bot is defined as a computer or internet-connected device that is infected with malware and controlled by a central command-and-control (C2) server. A botnet is the term used for all devices controlled by the C2 server, and they can be used to carry out large scale distributed denial of service (DDoS) attacks against websites, resulting in an overload of traffic on the website that renders it unusable.").

3. *See* Daniel Burrus, *The Internet of Things Is Far Bigger Than Anyone Realizes*, WIRED, https://www.wired.com/insights/2014/11/the-internet-of-things-bigger/ (last visited Feb. 4, 2021); Lawrence J. Trautman, *Cybersecurity: What About U.S. Policy?*, 2015 U. ILL. J.L. TECH. & POL'Y 341, 347–48 (2015).

4. Garrett M. Graff, *How a Dorm Room Minecraft Scam Brought Down the Internet*, WIRED (Dec. 13, 2017, 3:55 PM), https://www.wired.com/story/mirai-botnet-minecraft-scam-brought-down-the-internet/.

5. *Id.*

6. *Id.* This episode is analyzed in greater detail in SCOTT J. SHACKELFORD, THE INTERNET OF THINGS: WHAT EVERYONE NEEDS TO KNOW (2020).

7. *See* Charlie Osborne, *The Future of IoT? State-Sponsored Attacks, Say Security Professionals*, ZDNET (Aug. 13, 2018, 7:15 PM), https://www.zdnet.com/article/the-future-of-iot-state-sponsored-attacks-say-security-professionals/.

8. *Id.*

9. *See* Chris Welch, *Tesla's Model S Will Add Self-Driving 'Autopilot' Mode in Three Months*, VERGE (Mar. 19, 2015, 12:41 PM), http://www.theverge.com/2015/3/19/8257933/tesla-model-s-autopilot-release-date.

far smaller and cheaper—security cameras, baby monitors, kids' toys, doorbells, and even devices implanted in our own bodies, along with building controls, down to individual light bulbs. However, it remains unclear whether security—and privacy—can or will scale along with this increasingly crowded and interconnected marketplace or whether a combination of perverse incentives, increasing complexity, and new impacts of old problems like the "technical debt" amassing from products being rushed to market, or simple ignorance of security fundamentals on the part of manufactures or users, will derail progress and exacerbate prevalent cyber insecurity.[10] This is a particular problem for governments seeking to protect vulnerable IoT devices and networks in an array of critical infrastructure contexts, including healthcare and the electric grid, from foreign exploitation.[11]

The Mirai botnet episode noted above highlights the complexities involved in managing the multi-faceted cyber threat facing the public and private sectors. IoT botnets are concerning given that they provide state and non-state actors alike—including cybercriminals, politically motivated hacktivists, kids playing around, and nation-states[12]—asymmetric capabilities that can be used to target intellectual property and critical infrastructure. An array of public-private efforts, such as the National Institute for Standards and Technology (NIST) Cybersecurity Framework, efforts by civil society, such as the Consumer Reports *Digital Standard*, and national governments, such as the United Kingdom's Cyber Essentials Plus Certificate discussed in Parts II and III, are all being pursued to help harden the IoT. But will they be enough? What are the benefits and drawbacks of the various private and public IoT governance models being pursued by the EU and United States?[13] How much convergence is there among approaches purporting to govern the IoT, and what does that portend for the future of impacted industries and consumers, particularly given concerns over deepening digital divides driven in part by debates over 5G deployment?[14]

This Article focuses on cybersecurity standards set by industry, national governments, and international organizations, to make networks and network-connected devices more secure against hackers in general and, in particular, against politically motivated attacks by foreign governments, or their proxies.

---

10. This is an industry term for the legacy costs of rolling out new products without first improving security. *See* Taylor Armerding, *What Is Security Debt, and How Do I Get Out of It?*, SYNOPSYS (Mar. 16, 2020), https://www.synopsys.com/blogs/software-security/security-debt/; *see also Technical Debt*, TECHOPEDIA, https://www.techopedia.com/definition/27913/technical-debt (Mar. 20, 2017).

11. *See* Osborne, *supra* note 7.

12. Jason Kornwitz, *Why Politically Motivated Cyberattacks Might Be the New Normal*, PHYS.ORG (June 30, 2017), https://phys.org/news/2017-06-politically-cyberattacks.html ("[W]e'll 'certainly see more and more nation-state malware cropping up as cyberspace becomes more militarized as a way to achieve geopolitical goals.'").

13. China is another important epicenter for IoT governance but is not analyzed here due to space constraints. *See, e.g.*, Pan Qi, *China IoT Standards to Go Global*, CHINA DAILY (Jan. 4, 2018), http://www.chinadaily.com.cn/m/jiangsu/wuxi/2018-01/04/content_35441064.htm.

14. *See, e.g.*, Jeff John Roberts, *The Splinternet Is Growing*, FORTUNE (May 29, 2019, 3:30 AM), https://fortune.com/2019/05/29/splinternet-online-censorship/.

Such issues are at the forefront of both international business and geopolitics, with escalating tensions between the United States and Iran being a case in point of the stakes and vulnerabilities involved.[15] We investigate contemporary approaches to IoT security through an in-depth comparative case study focusing on the European Union (EU) and the United States, the first time that this has been attempted in the literature from a national security perspective.[16] Particular attention is paid to the impact of the General Data Protection Regulation (GDPR) and the Network Information Security (NIS) Directive in the EU, the influence of the NIST Cybersecurity Framework, and other leading technical standards and risk management strategies like cyber risk insurance, with a focus on mitigating the risk of politically motivated attacks.[17] We analyze transatlantic reform proposals and apply lessons from major Internet governance debates to argue for a polycentric approach to boosting IoT securing across both jurisdictions.

The Article is structured as follows. Part I introduces the topic with a brief history of the Internet of Things before moving on to reviewing prominent technical vulnerabilities and use cases, the argument over whether there is currently a market failure in the IoT context, and what role cyber risk insurance may play in mitigating it. Part II then focuses on the U.S. approach to IoT governance, paying particular attention to the federal regulatory landscape and relevant state initiatives along with the role played by civil society. Part III then analyzes EU efforts at IoT cybersecurity in some detail, paying particular attention to GDPR and including a national case study in the form of the United Kingdom (UK) and the impact of Brexit on its cybersecurity efforts. Part IV then

15. *Cf.* Jacquelyn Schneider, *It's Time to Calibrate Fears of a Cyberwar with Iran*, N.Y. TIMES (Jan. 7, 2020), https://www.nytimes.com/2020/01/07/opinion/iran-cyber-attack-hacking.html (making the case that large-scale cyber attacks on the United States from Iran are more difficult than is often reported).

16. *Cf.* Jane E. Kirtley & Scott Memmel, *Rewriting the "Book of the Machine": Regulatory and Liability Issues for the Internet of Things*, 19 MINN. J.L. SCI. & TECH. 455, 458–59 (2019) (surveying the field of IoT security with a focus on liability); Jenna Lindqvist, *New Challenges to Personal Data Processing Agreements: Is the GDPR Fit to Deal with Contract, Accountability and Liability in a World of the Internet of Things?*, 26 INT'L J.L. & INFO. TECH. 45, 59–61 (2018) (surveying GDPR as it applies to IoT governance with a particular focus on liability); Mauricio Paez & Mike La Marca, *The Internet of Things: Emerging Legal Issues for Business*, 43 N. KY. L. REV. 29, 68 (2016) (offering a speculative account of the impact of GDPR on IoT governance); Michael L. Rustad, *How the EU's General Data Protection Regulation Will Protect Consumers Using Smart Devices*, 52 SUFFOLK U. L. REV. 227, 244 (2019) (focusing on the impact of GDPR on consumer-focused IoT cybersecurity from an EU perspective); Jeremy Siegel, *When the Internet of Things Flounders: Looking into GDPR-esque Security Standards for IoT Devices in the United States from the Consumers' Perspective*, 20 J. HIGH TECH. L. 189, 194–95 (2020) (analyzing how GDPR would apply to IoT cybersecurity in the U.S. context); Charlotte A. Tschider, *Regulating the Internet of Things: Discrimination, Privacy, and Cybersecurity in the Artificial Intelligence Age*, 96 DENV. L. REV. 87, 130–31 (2019) (taking a high-level view of IoT governance with an emphasis on the emerging role of AI).

17. Of particulate note is the July 16, 2020 ruling from the European Court of Justice that found Privacy Shield unconstitutional, impacting the transatlantic data governance regime but upholding standard contractual clauses. As of this writing, the European Commission and the U.S. Department of Commerce have begun a new round of negotiation to replace Privacy Shield with a new regime consistent with the July 2020 ECJ ruling. Natasha Lomas, *EU-US Privacy Shield Is Dead. Long Live Privacy Shield*, TECHCRUNCH (Aug. 11, 2020, 2:21 AM), https://techcrunch.com/2020/08/11/eu-us-privacy-shield-is-dead-long-live-privacy-shield/.

summarizes policy implications both by applying lessons from the case studies to create an original spectrum of IoT governance by relying on lessons from the field of polycentric governance, and also taking lessons from the history of Internet governance and applying them to hot topics in IoT security including the emerging norm of cybersecurity due diligence.

I. WELCOME TO THE INTERNET OF EVERYTHING

It remains unclear where exactly the term "Internet of Things" (IoT) originated,[18] though it is without question that the term today is widely used to refer generally to a host of efforts to make our governments, businesses, and even our bodies, increasingly interconnected and hence, to some degree, "smart."[19] It features a wide range of products that "can be monitored, controlled[,] and linked"[20] together. Yet the positive press from such devices can hide their direct and indirect costs,[21] including the possibility of using them in situations of domestic abuse.[22] Moreover, public awareness of IoT remains low. One survey, for example, found that only twenty-five percent of respondents could define the "Internet of Things."[23] The decision to purchase a smart speaker or doorbell, for example, is rarely situated as part of a larger framework about the vulnerabilities it could introduce both personally, as well as in the wider community, similar to how many of us do not connect the use of disposable bags, or mining bitcoin, to marine or air pollution.[24] And for those who are in the trenches, it is not uncommon for "cyber fatigue" to set in. James Lewis of the Center for Strategic and International Studies, for example, has said, "[w]e have a faith-based approach [to cybersecurity], in that we pray every night that

18. Kevin Ashton, *That 'Internet of Things' Thing*, RFID J. (June 22, 2009), www.rfidjournal.com/articles/view?4986.

19. *See, e.g.*, Meghan Neal, *The Internet of Bodies Is Coming, and You Could Get Hacked*, VICE (Mar. 13, 2014, 11:20 AM), https://www.vice.com/en/article/gvyqgm/the-internet-of-bodies-is-coming-and-you-could-get-hacked; Hung LeHong & Jackie Fenn, *Hype Cycle for Emerging Technologies, 2011*, GARTNER (July 28, 2011), https://www.gartner.com/doc/1754719/.

20. Bonnie Cha, *A Beginner's Guide to Understanding the Internet of Things*, VOX (Jan. 15, 2015, 6:00 AM), https://www.vox.com/2015/1/15/11557782/a-beginners-guide-to-understanding-the-internet-of-things.

21. *See* Aaron Tilley, *How Hackers Could Use a Nest Thermostat as an Entry Point into Your Home*, FORBES (Mar. 6, 2015, 6:00 AM), https://www.forbes.com/sites/aarontilley/2015/03/06/nest-thermostat-hack-home-network/#235d0d693986; Carl Franzen, *How to Find a Hack-Proof Baby Monitor*, LIFEHACKER (Aug. 4, 2017, 6:30 PM), https://offspring.lifehacker.com/how-to-find-a-hack-proof-baby-monitor-1797534985; Charlie Osborne, *Smartwatch Security Fails to Impress: Top Devices Vulnerable to Cyberattack*, ZDNET (July 22, 2015, 10:25 PM), http://www.zdnet.com/article/smartwatch-security-fails-to-impress-top-devices-vulnerable-to-cyberattack/; John Markoff, *Why Light Bulbs May Be the Next Hacker Target*, N.Y. TIMES (Nov. 3, 2016), https://www.nytimes.com/2016/11/03/technology/why-light-bulbs-may-be-the-next-hacker-target.html.

22. *See* Nellie Bowles, *Thermostats, Locks and Lights: Digital Tools of Domestic Abuse*, N.Y. TIMES (June 23, 2018), https://www.nytimes.com/2018/06/23/technology/smart-home-devices-domestic-abuse.html.

23. *Infographic: IoT Awareness Is Low but Adoption Continues to Grow*, IOT TIMES (June 20, 2019), https://iot.eetimes.com/infographic-iot-awareness-is-low-but-adoption-continues-to-grow/.

24. *See IoT Is Coming Even if the Security Isn't Ready: Here's What to Do*, WIRED, https://www.wired.com/brandlab/2017/06/iot-is-coming-even-if-the-security-isnt-ready-heres-what-to-do/ (last visited Feb. 4, 2021).

nothing bad will happen."[25] In short, managing the growth of IoT impacts a diverse set of interests from national security to economic competitiveness, sustainable development, and trust in the digital age. How did we get here?

A. HISTORICAL DEVELOPMENT

The notion of deploying and leveraging the power of smart devices has been a goal decades in the making. Such "intelligent" devices were envisioned as far back as the 1950s and 1960s.[26] This trend continued during the creation of ARPANET, an undertaking that eventually became what we refer to as the Internet, under the heading of "pervasive computing."[27] For example, Carnegie-Mellon University researchers in the 1980s deployed sensors in a vending machine.[28] By the 1990s, even though the Internet was increasingly global, slow connection speeds held back IoT devices and services.[29]

The potential of IoT tech has arguably only been realized since 2010,[30] the result of the confluence of at least three factors: (1) the widespread availability of always-on high-speed Internet connectivity in many parts of the world; (2) faster computational capabilities permitting the real-time analysis of Big Data; and (3) economies of scale lowering the cost of sensors and chips to manufacturers.[31] However, the rapid rollout of IoT technologies has not been accompanied by any mitigation of the array of technical vulnerabilities across these devices, which are introduced next.

B. TECHNICAL VULNERABILITIES AND USE CASES

As has often been observed, the Internet was not designed with security in mind.[32] Access to the early ARPANET was restricted to government-funded

---

25. Ken Dilanian, *Privacy Group Sues to Get Records About NSA-Google Relationship*, L.A. TIMES (Sept. 14, 2010, 12:00 AM), https://www.latimes.com/archives/la-xpm-2010-sep-14-la-fi-nsa-google-20100914-story.html.

26. *See* NILS J. NILSSON, THE QUEST FOR ARTIFICIAL INTELLIGENCE: A HISTORY OF IDEAS AND ACHIEVEMENTS 71 (2010).

27. LeHong & Fenn, *supra* note 19.

28. *The Internet of Things: Groundbreaking Tech with Security Risks*, WELIVESECURITY (Oct. 29, 2015, 12:49 PM), http://www.welivesecurity.com/2015/10/29/internet-things-groundbreaking-tech-security-risks/ ("Researchers at Carnegie Mellon University first came up with an internet-connected Coke vending machine in 1982.").

29. *See, e.g.*, Steve Ranger, *What Is the IoT? Everything You Need to Know About the Internet of Things Right Now*, ZDNET (Feb. 3, 2020, 6:45 PM), https://www.zdnet.com/article/what-is-the-internet-of-things-everything-you-need-to-know-about-the-iot-right-now/.

30. *See* Jacob Morgan, *A Simple Explanation of 'The Internet of Things'*, FORBES (May 13, 2014, 12:05 AM), http://www.forbes.com/sites/jacobmorgan/2014/05/13/simple-explanation-internet-things-that-anyone-can-understand/.

31. *See* JIM CHASE, THE EVOLUTION OF THE INTERNET OF THINGS, TEX. INSTRUMENTS (2013), www.ti.com/lit/ml/swrb028/swrb028.pdf; Scott J. Shackelford, Anjanette Raymond, Danuvasin Charoen, Rakshana Balakrishnan, Prakhar Dixit, Julianna Gjonaj, & Rachith Kavi, *When Toasters Attack: A Polycentric Approach to Enhancing the "Security of Things"*, 2017 U. ILL. L. REV. 415, 422 (2017).

32. Craig Timberg, *A Flaw in the Design*, WASH. POST (May 30, 2015), https://www.washingtonpost.com/sf/business/2015/05/30/net-of-insecurity-part-1/.

researchers and, even after more than a decade, fewer than a thousand computers were connected to it.[33] With a limited and controlled set of users, security was not considered an important issue. Thus, the underlying architecture and protocols of the Internet do not have security "built-in."[34]

Because the network itself does not provide adequate security protections, security is left to the devices connected to the network, which are often not up to the task. This includes toasters, which in many ways have become the quintessential example of an Internet-connected device that, perhaps, should not be.[35] Former Director of National Intelligence, James Clapper, for example, has warned about the vulnerabilities in various IoT devices, including toasters, to be utilized by intelligence agencies around the world to aid surveillance efforts.[36] Too many device or software vendors have been slow to understand that it is the vendor's job to provide security in the systems they sell. For example, it was not until early 2002 that Microsoft, the primary vendor of operating system software for Internet-connected devices, made security a primary goal.[37] To this day, far too many medical devices have inadequate security.[38] Industrial controllers are often vulnerable because vendors incorrectly assumed they would only be used on isolated networks, not the Internet.[39] Too many IoT toys and devices, such as security cameras and baby monitors, have fixed and unchangeable access passwords which, when (not if) discovered, open the devices to exploitation.[40] This is now easily done by making use of websites such as Shodan, which can allow anyone (hackers and defenders alike) to search for IoT devices connected to the Internet.[41] Many IoT devices are built using embedded computing modules that were programmed by component manufacturers who,

33. Robert H. Zakon, *Hobbes' Internet Timeline*, ZAKON, https://www.zakon.org/robert/internet/timeline/ (Jan. 1, 2018).

34. Timberg, *supra* note 32.

35. *See* Alex Hern & Arwa Mahdawi, *Beware the Smart Toaster: 18 Tips for Surviving the Surveillance Age*, GUARDIAN (Mar. 28, 2018), https://www.theguardian.com/technology/2018/mar/28/beware-the-smart-toaster-18-tips-for-surviving-the-surveillance-age.

36. *See* Steve Ranger, *Yes, Your Smart Toaster Really Will Be Spying on You for the Government*, ZDNET (Feb. 12, 2016, 4:47 PM), https://www.zdnet.com/article/yes-your-smart-toaster-really-will-be-spying-on-you-for-the-government/ ("In the future, intelligence services might use the IoT for identification, surveillance, monitoring, location tracking, and targeting for recruitment, or to gain access to networks or user credentials.").

37. Bill Gates, *Bill Gates: Trustworthy Computing*, WIRED (Jan. 17, 2002, 12:00 PM), https://www.wired.com/2002/01/bill-gates-trustworthy-computing/.

38. Lily Hay Newman, *Medical Devices Are the Next Security Nightmare*, WIRED (Mar. 2, 2017, 10:30 AM), https://www.wired.com/2017/03/medical-devices-next-security-nightmare/; Scott J. Shackelford, Michael Mattioli, Steve Myers, Austin Brady, Yvette Wang, & Stephanie Wong, *Securing the Internet of Healthcare*, 19 MINN. J.L. SCI. & TECH. 405 (2018); Kelly Sheridan, *Severe Vulnerabilities Discovered in GE Medical Devices*, DARK READING (Jan. 23, 2020, 1:40 PM), https://www.darkreading.com/threat-intelligence/severe-vulnerabilities-discovered-in-ge-medical-devices/d/d-id/1336867.

39. Robert Abel, *Researchers Find 147 Vulnerabilities in 34 SCADA Mobile Applications*, SC MEDIA (Jan. 11, 2018), https://www.scmagazine.com/the-top-security-weaknesses-were-code-tampering-flaws-which-were-found-in-94-percent-of-apps/article/736656/.

40. Anna Bryk, *IoT Toys: A New Vector for Cyber Attacks*, APRIORIT (Feb. 2, 2018, 7:18 PM), https://www.apriorit.com/dev-blog/521-iot-toy-attacks.

41. *See* SHODAN, https://www.shodan.io/ (last visited Feb. 4, 2021).

demonstrably, have little to no security expertise.[42] Moreover, even more sophisticated firms have run into trouble. Amazon's Ring smart doorbell, for example, has been the subject of a federal class action investigation after breaches due to alleged lax security such as a lack of multi-factor authentication.[43] This begs the question of whether or not there is a market failure when it comes to IoT security.

C. AN IOT MARKET FAILURE?

Debates have played out for years over whether or not there is a market failure in the cybersecurity context generally, or in IoT specifically.[44] Market failures occur when price mechanisms fail to take account of the relevant "costs and benefits necessary to provide and consume a good,"[45] such as when the stock prices of firms are not negatively impacted following a data breach even as their customers and employees suffer.[46] Relatedly, as applied to IoT, Yosef Yudborovsky has argued, "[t]he security failure at the heart of IoT is a product of the lack of incentives owners see in defining the software to provide its maximum security."[47] In short, such a limited perspective can result not only in more frequent exploitations and data breaches, but also in perpetuating identity theft and potentially exacerbating national security concerns. A future could play out wherein some consumers who can afford the added cost are able to enjoy the benefits of more secure (and thereby private) devices, whereas others who are less well-off are forced to rely on insecure products.

There are important ethical and legal implications of such an IoT market failure worth exploring. For example, under a utilitarian framing, the costs to society generally are high in a hyper-connected IoT ecosystem powering a surveillance economy in which a reasonable expectation of personal privacy becomes technically impossible, in either public or private settings.[48] There are

---

42. Darren Allan, *Dangerous Backdoor Exploit Found on Popular IoT Devices*, TECHRADAR (Mar. 2, 2017), https://www.techradar.com/news/dangerous-backdoor-exploit-found-on-popular-iot-devices.

43. *E.g.*, *Amazon's Ring Slammed with Federal Lawsuit*, CISO MAG. (Dec. 30, 2019), https://www.cisomag.com/amazons-ring-slammed-with-federal-lawsuit/ ("According to researchers, the vulnerability stems from when the Ring smartphone app sends the wireless network connections to the Amazon Ring servers in the cloud. It's found that this process is taking place in an insecure manner, which can be exploited by an attacker.").

44. *See* Eli Dourado, *Is There a Cybersecurity Market Failure?* 19–33 (George Mason Univ. Mercatus Ctr., Working Paper No. 12-05, 2012), https://www.mercatus.org/system/files/Cybersecurity_Dourado_WP1205_0.pdf (arguing that market failures are not so common in the cybersecurity realm); Jerry Brito & Tate Watkins, *Loving the Cyber Bomb? The Dangers of Threat Inflation in Cybersecurity Policy*, 3 HARV. NAT'L SEC. J. 39, 82 (2011) (making the case against there being a cybersecurity market failure).

45. *Introducing Market Failure*, LUMEN LEARNING: BOUNDLESS ECON., https://courses.lumenlearning.com/boundless-economics/chapter/introducing-market-failure/ (last visited Feb. 4, 2021).

46. *See* Shinichi Kamiya, Jun-Koo Kang, Jungmin Kim, Andreas Milidonis & René M. Stulz, *What Is the Impact of Successful Cyberattacks on Target Firms?* 31 (Nat'l Bureau of Econ. Rsch., Working Paper No. 24409, 2018), https://www.nber.org/system/files/working_papers/w24409/w24409.pdf.

47. Yosef Yudborovsky, *The Failure in the Market for the Internet of Things*, MEDIUM (June 27, 2017), https://medium.com/@yoss202/the-failure-in-the-market-for-internet-of-things-cff948f571b9.

48. SHACKELFORD, *supra* note 6, at ch. 4.

several ways to leverage the market to avoid such an Orwellian outcome, some of which are explored in Parts II through IV. For example, civil society may be leveraged to better inform consumers about the security traits of the products they are considering (such as the Consumer Reports *Digital Standard*). IoT trustmarks and certification schemes may be utilized to a similar end. IoT product manufacturers may also be compelled to internalize the costs of their insecure products, as seen in California and the EU.[49] More generally, firms could recognize IoT security not only as a necessary cost of doing business, but as a corporate social responsibility.[50]

Regrettably, we shall see the U.S. government has been slow to address the situation despite occasional calls for a "shared responsibility" in promoting cybersecurity.[51] As a result, these devices have been left open to exploitation, necessitating a new approach to IoT governance that would include a role for insurance as part of a larger polycentric approach to securing IoT.

D. CONSIDERING A ROLE FOR INSURANCE

Interconnected devices have the potential to drive numerous new businesses, and even industries, but they also contribute to our collective cyber insecurity. An increasingly popular tool to help mitigate the risk of cyber attacks is insurance, with total global premiums being on the order of $20 billion by 2025.[52] The value of the U.S. market alone for cyber risk insurance is expected to surpass $3 billion by 2025, with more than 40% of small and medium-sized enterprises (SMEs), and greater than 60% of large enterprises, having cyber risk coverage in 2019.[53] Target, for example, was able to recover $44 million from its insurance carrier following its massive data breach in 2013–2014.[54] Indeed, a growing number of public sector stakeholders—including local governments and even state agencies—are purchasing cyber risk insurance policies to help mitigate the risks they face.[55]

However, there are myriad problems associated with cyber attacks that insurance is either ill-suited or unable to help manage. For example, it has long been the case that it is difficult to purchase insurance coverage for trade secrets, impacts on brand or reputation following a data breach, or other hard-to-quantify

49. *See infra* Parts II–IV.

50. For more on this topic, see Scott J. Shackelford, Timothy L. Fort & Danuvasin Charoen, *Sustainable Cybersecurity: Applying Lessons from the Green Movement to Managing Cyber Attacks*, 2016 U. ILL. L. REV. 1995 (2016).

51. Rand Beers, *Cybersecurity: A Shared Responsibility*, DEP'T HOMELAND SEC. (Oct. 18, 2013, 1:33 PM), https://www.dhs.gov/blog/2013/10/18/cybersecurity-shared-responsibility.

52. Jennifer Rudden, *Cyber Insurance—Statistics & Facts*, STATISTA (Sept. 24, 2019), https://www.statista.com/topics/2445/cyber-insurance/.

53. *Id.*

54. Dhanya Skariachan & Jim Finkle, *Target's Cyber Insurance Softens Blow of Massive Credit Breach*, INS. J. (Feb. 26, 2014), https://www.insurancejournal.com/news/national/2014/02/26/321638.htm.

55. *See, e.g.*, Scott Ikeda, *Cyber Insurance Now Critical for Public Sector Agencies?*, CPO MAG. (Nov. 29, 2017), https://www.cpomagazine.com/cyber-security/cyber-insurance-now-critical-public-sector-agencies/.

costs.[56] This fact is problematic given that the vast majority of the firms comprising the S&P 500 are tied up in intangible assets, namely intellectual property.[57] Moreover, numerous organizations that think they are covered for a given cyber incident have found out otherwise in the aftermath of a breach given how these policies can be written with exclusions for various first- and third-party losses, not to mention acts of cyber war and terrorism.[58] For the latter, as of this writing Maersk is litigating with its insurance carrier over whether or not the $1.3 billion in losses it sustained in June 2017 is covered by its insurance policy given that it was likely Russia's military intelligence agency behind the breach.[59] This facet of many existing policies limits the utility of cyber risk insurance to help mitigate the risk of politically motivated cyber attacks utilizing IoT vulnerabilities.

Indeed, IoT is challenging for cyber risk insurance providers on several fronts, including the fact of how difficult it is to quantify the risk given how many of these smart products lack "even basic . . . security features . . . such as updates and patches."[60] Adding this to the fact that cyber attacks on IoT devices, such as pacemakers or furnaces, can have real-world and even life-threatening impacts means that more people, and organizations, will see this as vital to mitigating cyber risks.[61] However, building actuarial tables to better understand the IoT cyber threat landscape is no simple matter given the relative lack of verifiable data.[62] Clearly, then, IoT cyber risk insurance coverage will be an increasingly popular, if still incomplete and problematic, component of a polycentric approach to managing the full range of cyber threats threating individuals, organizations, and nations.

E. A POLYCENTRIC APPROACH TO SECURING IOT

Of the many ways to consider cybersecurity policy in the IoT context, among the most potentially helpful is arguably polycentric governance. As has

56. *See, e.g.*, Christine Marciano, *Trade Secrets Are Not Covered by Cyber Insurance*, DATA BREACH INS. (Feb. 21, 2013), https://databreachinsurancequote.com/cyber-insurance/trade-secrets-are-not-covered-by-cyber-insurance/.

57. *See* Bruce Berman, *$21 Trillion in U.S. Intangible Assets Is 84% of S&P 500 Value—IP Rights and Reputation Included*, IP CLOSEUP (June 4, 2019), https://ipcloseup.com/2019/06/04/21-trillion-in-u-s-intangible-asset-value-is-84-of-sp-500-value-ip-rights-and-reputation-included/.

58. *See* Scott J. Shackelford & Scott Russell, *Risky Business: Lessons for Mitigating Cyber Attacks from the International Insurance Law on Piracy*, 24 MINN. J. INT'L L. 1, 1–3 (2015); Scott J. Shackelford, *Should Your Firm Invest in Cyber Risk Insurance?*, 55 BUS. HORIZONS 349, 353–54 (2012).

59. *See* Riley Griffin, Katherine Chiglinsky & David Voreacos, *Was It an Act of War? That's Merck Cyber Attack's $1.3 Billion Insurance Question*, INS. J. (Dec. 3, 2019), https://www.insurancejournal.com/news/national/2019/12/03/550039.htm (noting that the real targets behind NotPetya were in Ukraine and Maersk was "collateral damage").

60. MARSH & MCLENNON COS., THE INTERNET OF EVERYTHING: BUILDING CYBER RESILIENCE IN A CONNECTED WORLD 2 (2018), https://www.marsh.com/us/insights/research/building-cyber-resilience-in-a-connected-world.html (select "view full article").

61. *See id.* at 3–5.

62. *See* Doffman, *supra* note 1.

been previously argued, this framework "is a multi-level, multi-purpose, multi-functional, and multi-sectoral model"[63] that "challenges orthodoxy [in part] by demonstrating the benefits of self-organization [and] networking regulations 'at multiple scales.'"[64] Polycentricity also argues for a set of nested stakeholders rather than "a single governmental unit," which is often unable to address "global collective action problems"[65] such as cyber-attacks in the IoT context. This approach, in other words, "recognizes both the common but differentiated responsibilities of public- and private-sector stakeholders as well as the potential for best practices to be identified and spread organically, generating positive network effects that could, in time, result in the emergence of a cascade toward a cybersecurity due diligence norm."[66]

Elinor Ostrom's seminal book *Governing the Commons* offered a series of eight design principles distilled from her extensive fieldwork for the effective management of common pool resources (CPRs).[67] IoT security has been equated to a CPR problem,[68] and if true, Ostrom's principles[69] may prove helpful in making predictions about the governance of various regimes under differing scenarios. These include the importance of: (1) "clearly defined boundaries for the user pool . . . and the resource domain";[70] (2) "[p]roportional equivalence between benefits and costs";[71] (3) "[c]ollective choice arrangements" ensuring "that the resource users participate in setting . . . rules";[72] (4) "[m]onitoring . . . by the appropriators or by their agents";[73] (5) "[g]raduated

63. Scott J. Shackelford, *The Law of Cyber Peace*, 18 CHI. J. INT'L L. 1, 7 (2017) (citing Michael D. McGinnis, *An Introduction to IAD and the Language of the Ostrom Workshop: A Simple Guide to a Complex Framework*, 39 POL'Y STUD. J. 169, 171–72 (2011) ("Polycentricity is a system of governance in which authorities from overlapping jurisdictions (or centers of authority) interact to determine the conditions under which these authorities, as well as the citizens subject to these jurisdictional units, are authorized to act as well as the constraints put upon their activities for public purposes.").

64. *Id.* (quoting Elinor Ostrom, *Polycentric Systems as One Approach for Solving Collective-Action Problems* 1 (Ind. Univ. Workshop in Pol. Theory and Pol'y Analysis & Ariz. State Univ. Ctr. for the Study of Inst. Diversity, Working Paper No. 08-6, 2008), http://dlc.dlib.indiana.edu/dlc/bitstream/handle/10535/4417/W08-6_Ostrom_DLC.pdf?sequence=1).

65. Elinor Ostrom, *A Polycentric Approach for Coping with Climate Change* 35 (Dev. & Econ. Rsch. Grp., World Bank, Policy Research Working Paper No. 5095, 2009), https://openknowledge.worldbank.org/bitstream/handle/10986/9034/WPS5095_WDR2010_0021.pdf?sequence=1&isAllowed=y.

66. Scott J. Shackelford, Scott Russell & Andreas Kuehn, *Unpacking the International Law on Cybersecurity Due Diligence: Lessons from the Public and Private Sectors*, 17 CHI. J. INT'L L. 1, 47 (2016) (citing Martha Finnemore & Kathryn Sikkink, *International Norm Dynamics and Political Change*, 52 INT'L ORG. 887, 895–98 (1998)). For a deeper dive on this topic, see chapter 2 of SCOTT J. SHACKELFORD, MANAGING CYBER ATTACKS IN INTERNATIONAL LAW, BUSINESS, AND RELATIONS: IN SEARCH OF CYBER PEACE (2014).

67. *See* ELINOR OSTROM, GOVERNING THE COMMONS: THE EVOLUTION OF INSTITUTIONS FOR COLLECTIVE ACTION 90 (1990); *see also* SUSAN J. BUCK, THE GLOBAL COMMONS: AN INTRODUCTION 5 (1998).

68. *See* Isaac Kohen, *Why IoT Device Security Is a Common Pool Resource*, IOT WORLD TODAY (Apr. 9, 2018), https://www.iotworldtoday.com/2018/04/09/why-iot-device-security-common-pool-resource/.

69. *See* Elinor Ostrom, Beyond Markets and States: Polycentric Governance of Complex Economic Systems, Nobel Prize Lecture (Dec. 8, 2009), *in* 100 AM. ECON. REV. 641, 653 (2010).

70. BUCK, *supra* note 67, at 32.

71. Ostrom, *supra* note 64, at 13.

72. BUCK, *supra* note 67, at 32.

73. *Id.*

sanctions" for rule violators;[74] (6) "[c]onflict-resolution mechanisms [that] are readily available, low cost, and legitimate";[75] (7) "[m]inimal recognition of rights to organize";[76] and (8) "governance activities [being] organized in multiple layers of nested enterprises."[77]

It should be apparent that not all of Professor Ostrom's design principles are equally applicable in the IoT context. For example, boundaries in the IoT context are relatively fluid depending on the governance level at issue, and thus may be difficult to draw and enforce.[78] Another instance is Professor Ostrom's third design principle, which states "that most of the individuals affected by a resource regime are authorized to participate in making and modifying the rules related to boundaries, assessment of costs . . . etc."[79] This principle calls for proactive rulemaking by various stakeholders, including technical communities.[80] The history of Internet governance has been marked by such a multi-stakeholder approach to governance, as is discussed further in Part IV. Moreover, this principle recognizes the need for dynamic rules that keep pace with a changing regulatory and technological environment.[81] One example of this practice being manifest has been the rollout and wide adoption of the NIST CSF, which is helping to establish a baseline of cybersecurity due diligence from the bottom up both in the United States and around the world.[82]

Other theorists have also pioneered work relevant to this discussion, which has been discussed at length in previous works but is worth introducing here.[83] Professor Yochai Benkler, for example, conceptualized a three-layer structure of cyberspace, including: (1) the "physical infrastructure," including the routers

---

74. *Id.*

75. *Id.*

76. Elinor Ostrom, *Polycentric Systems: Multilevel Governance Involving a Diversity of Organizations*, *in* GLOBAL ENVIRONMENTAL COMMONS: ANALYTICAL AND POLITICAL CHALLENGES IN BUILDING GOVERNANCE MECHANISMS 105, 118 tbl.5.3 (Eric Brousseau, Tom Dedeurwaerdere, Pierre-André Jouvet & Marc Willinger eds., 2012).

77. *Id*.

78. *See* ANDREW W. MURRAY, THE REGULATION OF CYBERSPACE: CONTROL IN THE ONLINE ENVIRONMENT 164 (2007) (explaining how members of micro-communities tend to focus only on what directly impacts their own activities).

79. Ostrom, *supra* note 76, at 120.

80. *See* George J. Siedel & Helena Haapio, *Using Proactive Law for Competitive Advantage*, 47 AM. BUS. L.J. 641, 656–57 (2010) (discussing the origins of the proactive law movement, which may be considered "a future-oriented approach to law placing an emphasis on legal knowledge to be applied before things go wrong" (quoting NORDIC SCHOOL OF PROACTIVE LAW, http://www.juridicum.su.se/proactivelaw/main/)).

81. Ostrom, *supra* note 76, at 120.

82. *See* Scott J. Shackelford, Andrew A. Proia, Brenton Martell & Amanda N. Craig, *Toward a Global Cybersecurity Standard of Care?: Exploring the Implications of the 2014 NIST Cybersecurity Framework on Shaping Reasonable National and International Cybersecurity Practices*, 50 TEX. INT'L L.J. 305, 309–10 (2015); Scott J. Shackelford, Scott Russell, & Jeffrey Haut, *Bottoms Up: A Comparison of "Voluntary" Cybersecurity Frameworks*, 16 U.C. DAVIS BUS. L.J. 217, 219, 222–23 (2016) [hereinafter Shackelford et al., *Bottoms Up*].

83. *See generally* Scott J. Shackelford, *Toward Cyberpeace: Managing Cyber Attacks Through Polycentric Governance*, 62 AM. U. L. REV. 1273 (2013) (discussing the different governance models proposed by theorists and their security implications).

and smart devices that comprise the physical aspect of cyberspace and IoT; (2) the "logical infrastructure," including the TCP/IP protocol; and (3) the "content layer," which incorporates data and, indirectly, users.[84] This model is similar to Professor Lawrence Lessig's model from his 1999 book on how code becomes law,[85] which also advocated for protecting openness and "decentralized innovation."[86] However, Professor Andrew Murray has criticized this approach as being too "idealistic," stating that "the harnessing of one regulatory modality through the application of another is more likely to lead to further regulatory competition, due to the complexity of the network environment."[87] Instead of a single approach, though, Professor Lessig identified four modalities of cyber regulation: architecture, law, the market, and norms that "may be used individually or collectively" by policymakers seeking to enhance IoT security.[88]

The following Part digs more deeply into how two principal cyber powers—the United States and the EU—have leveraged these modalities to address latent IoT insecurity. As will be apparent, despite having much in common, these two jurisdictions have addressed IoT governance quite differently, with the EU preferring a more comprehensive, regulatory approach as compared to the more sector-specific, standards-based U.S. approach. Still, both regimes have similarities, which can be leveraged to help build momentum toward new international cybersecurity due diligence norms focused on securing smart devices.

II. U.S. CASE STUDY

The United States, long a pioneer in Internet technologies and their application, has increasingly focused on the promise and peril of IoT technologies, including the ways in which they could be leveraged for politically motivated hacking. This Part unpacks the current U.S. regulatory framework pertaining to IoT devices before moving to analyze reform efforts at the state and federal levels. We then discuss the utility of cybersecurity frameworks and standards, focusing on those published by NIST and Consumer Reports, to better understand whether these various modalities will be sufficient at helping to fill prevailing governance gaps.

---

84. Yochai Benkler, *From Consumers to Users: Shifting the Deeper Structure of Regulation Toward Sustainable Commons and User Access*, 52 FED. COMMC'NS L.J. 561, 562 (2000).

85. *See* LAWRENCE LESSIG, CODE AND OTHER LAWS OF CYBERSPACE (1999); *see also* LAWRENCE LESSIG, FREE CULTURE: HOW BIG MEDIA USES TECHNOLOGY AND THE LAW TO LOCK DOWN CULTURE AND CONTROL CREATIVITY 160 (2004) (describing "the interaction between architecture and law" in the context of copyright regulation).

86. LAWRENCE LESSIG, THE FUTURE OF IDEAS: THE FATE OF THE COMMONS IN A CONNECTED WORLD 85 (2002).

87. MURRAY, *supra* note 78, at 46 ("It is highly unlikely that content producers, media corporations and other copyright holders will allow for a neutral system designed to protect cultural property and creativity at the cost of loss of control over their products.").

88. *Id.* at 28.

A. FEDERAL REGULATORY LANDSCAPE

As stated above, the United States has favored a generally voluntary, sector-specific or topic-specific approach to both cybersecurity and data privacy. This is unlike the mandatory and comprehensive approach, the General Data Protection Regulation (GDPR), enacted in May 2018 in the EU, which came into force in May 2018.[89] In short, not all private data is created equal in the United States: it matters whether it is health or financial data, or your IP address or Internet searches (at least outside of California).[90] The latter, for example, are safeguarded by GDPR as personal data for EU citizens, but U.S. citizens do not enjoy similar protections.[91] Similarly, cybersecurity regulation in the United States—particularly in the IoT context—includes a patchwork of federal and state laws and policies, which are summarized below and compared in Part III to the EU.[92] In general, though, such protections are more robust in Europe than in the United States, ranging from heightened requirements to disclose cyber attacks to national authorities, cyber attack post-mortem requirements and requirements to appoint a Data Protection Officer to enhanced consent requirements, as discussed further below.[93] Such standards would not protect against all incidents of sophisticated foreign states targeting vulnerable networks, but they do help to raise the overall level of cybersecurity due diligence, as is discussed further in Part IV.

Due to both the scope and complexity inherent in the IoT, federal cybersecurity law has so far not been up to the task of mitigating security problems arising in this context.[94] Governance gaps remain common, despite the best efforts by groups such as the Federal Trade Commission (FTC), which encourages, but does not require, firms to:

1. [B]uild security into devices at the outset, rather than as an afterthought in the design process;
2. [T]rain employees about the importance of security, and ensure that security is managed at an appropriate level in the organization;

89. *See, e.g.*, Meghna Chakrabarti, *Overhauling Digital Privacy in the EU*, NPR: ON POINT, http://www.wbur.org/onpoint/2018/04/24/eu-gdpr-facebook-digital-privacy (Apr. 24, 2018).

90. *See* David Zetoony, *CCPA Privacy and Security FAQs: If a Company Receives a Right to Be Forgotten Request, Does It Have to Delete the Requestor's IP Address from Its Weblogs?*, JD SUPRA (Oct. 24, 2019), https://www.jdsupra.com/legalnews/ccpa-privacy-and-security-faqs-if-a-28543/ (explaining that it is an open question whether IP addresses are indeed covered).

91. *See What Is Personal Data?*, EU GDPR COMPLIANT, https://eugdprcompliant.com/personal-data/ (last visited Feb. 4, 2021).

92. *See* 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.

93. *Id.*

94. *See FTC Report on Internet of Things Urges Companies to Adopt Best Practices to Address Consumer Privacy and Security Risks*, FED. TRADE COMM'N (Jan. 27, 2015), https://www.ftc.gov/news-events/press-releases/2015/01/ftc-report-internet-things-urges-companies-adopt-best-practices.

3. [E]nsure that when outside service providers are hired, that those providers are capable of maintaining reasonable security, and provide reasonable oversight of the providers;
4. [W]hen a security risk is identified, consider a "defense-in-depth" strategy whereby multiple layers of security may be used to defend against a particular risk;
5. [C]onsider measures to keep unauthorized users from accessing a consumer's device, data, or personal information stored on the network;
6. [M]onitor connected devices throughout their expected life cycle, and where feasible, provide security patches to cover known risks.[95]

In sum, the FTC recommends "tackling data security and all consumer-facing software development efforts with a holistic approach that incorporates a 'privacy by design' strategy to address the entire life cycle of data collection, use, access, storage and ultimately secure data deletion."[96] These suggestions are in line with both the 2014 NIST Cybersecurity Framework and the 2015 NIST IoT Framework discussed next. They help to address the problem of politically motivated cyber attacks on IoT networks because they help to raise the overall level of cybersecurity due diligence, including for defense contractors, promoting defense-in-depth.[97]

The FTC has authority under Section 5 of the Federal Trade Commission Act to protect consumers from "unfair or deceptive acts or practices."[98] Over time, the FTC has engaged in enforcement actions against firms with inadequate cybersecurity safeguards, particularly those operating in a critical infrastructure context. The U.S. Court of Appeals for the Third Circuit upheld the FTC's authority to regulate cybersecurity in 2015.[99] However, based on a more recent case, *LabMD Inc. v. Federal Trade Commission*,[100] the FTC is being pushed to become more specific with regards to the cybersecurity standards it requires of covered U.S. businesses. In essence, the U.S. Court of Appeals for the Eleventh Circuit, to be consistent with the reference to the Third Circuit, ruled in June 2018 that, since the FTC had not provided specific cybersecurity standards

95. *Id.*

96. Richard Santalesa, *FTC Enters "Internet of Things" Arena with TRENDnet Proposed Settlement*, INFOLAWGROUP (Sept. 9, 2013), https://web.archive.org/web/20130917003715/https://www.infolawgroup.com/2013/09/articles/ftc/trendnet-settlement/.

97. *See* DEP'T OF HOMELAND SEC., RECOMMENDED PRACTICE: IMPROVING INDUSTRIAL CONTROL SYSTEM CYBERSECURITY WITH DEFENSE-IN-DEPTH STRATEGIES (2016), https://us-cert.cisa.gov/sites/default/files/recommended_practices/NCCIC_ICS-CERT_Defense_in_Depth_2016_S508C.pdf.

98. *A Brief Overview of the Federal Trade Commission's Investigative, Law Enforcement, and Rulemaking Authority*, FED. TRADE COMM'N, https://www.ftc.gov/about-ftc/what-we-do/enforcement-authority (last visited Feb. 4, 2021) (quoting 15 U.S.C. § 45(a)(1)).

99. W. Reece Hirsch, Rahul Kapoor, & Shokoh H. Yaghoubi, *Third Circuit Sides with FTC in Data Security Dispute with Wyndham*, NAT'L L. REV. (Sept. 8, 2015), https://www.natlawreview.com/article/third-circuit-sides-ftc-data-security-dispute-wyndham; *see also* Fed. Trade Comm'n v. Wyndham Worldwide Corp., 799 F.3d 236, 259 (3d Cir. 2015).

100. LabMD, Inc. v. Fed. Trade Comm'n, 678 F. App'x 816 (11th Cir. 2016).

defining reasonableness for LabMD, a now bankrupt cancer-screening company, the FTC's order was illegal.[101]

While not challenging the FTC's authority to police cybersecurity, the court did significantly tighten the grounds over which the FTC could initiate investigations and levy fines and settlement orders. Specifically, the underlying data breach must violate some specific law such as the Health Insurance Portability and Accountability Act of 1996 (HIPPA).[102] Thus, the FTC cannot penalize a company for the release of data causing a substantial consumer injury if it is not subject to an existing law. The Eleventh Circuit did not address whether the FTC's use of the negligence tort sufficed in this case. The FTC argued that "its enforcement action was grounded in the common law of negligence because LabMD unintentionally allowed the invasion of its customers' privacy."[103] To be clear, even though the Eleventh Circuit did not rule on that question here, a consumer harmed would still be able to seek damages under a negligence cause of action in common law, though that comes with its own challenges such as the economic loss doctrine.[104] In addition, depending on where the person resides there could also be the option of state-level relief. For example, California's 2018 Consumer Privacy Act, now in effect, is promoting higher standards for data use transparency.[105] It does not go as far as the EU's GDPR discussed in Part III, but it does include provisions that allow consumers to sue in the aftermath of data breaches including in the IoT context.[106] Moreover, as of January 2020, under California Senate Bill 327, "any manufacturer of a device that connects 'directly or indirectly' to the Internet must equip it with 'reasonable' security features, designed to prevent unauthorized access, modification, or information disclosure."[107] Yet these laws do little to regulate the importation of insecure IoT products from overseas,

101. Alison Frankel, *There's a Big Problem for the FTC Lurking in the 11th Circuit's LabMD Data-Security Ruling*, REUTERS (June 7, 2018, 1:39 PM), https://www.reuters.com/article/us-otc-labmd/theres-a-big-problem-for-the-ftc-lurking-in-11th-circuits-labmd-data-security-ruling-idUSKCN1J32S2.

102. *Id.*

103. *Id.*

104. *See, e.g.*, David W. Opderbeck, *Cybersecurity, Data Breaches, and the Economic Loss Doctrine in the Payment Card Industry*, 75 MD. L. REV. 935, 936–38 (2016).

105. *See* California Consumer Privacy Act of 2018, CAL. CIV. CODE § 1798.1 (2018); *see also* Devin Coldewey, *The California Consumer Privacy Act Officially Takes Effect Today*, TECHCRUNCH (Jan. 1, 2020, 6:01 AM), https://techcrunch.com/2020/01/01/the-california-consumer-privacy-act-officially-takes-effect-today/.

106. *See* Ben Adler, *California Passes Strict Internet Privacy Law with Implications for the Country*, NPR (June 29, 2018, 5:05 AM), https://www.npr.org/2018/06/29/624336039/california-passes-strict-internet-privacy-law-with-implications-for-the-country.

107. 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-cybersecurity-bill-sb-327-signed-law; *see also* Lindsey O'Donnell, *IoT Security Regulation Is on the Horizon*, THREAT POST (June 6, 2019, 8:44 AM), https://threatpost.com/iot-security-regulation-horizon/145406/ (noting that the law requires "reasonable security feature or features that are appropriate to the nature and function of the device").

which if enacted still would admittedly pose extraterritorial concerns of the kind surrounding GDPR discussed below.

There currently seems to be a growing circuit split over the FTC's cybersecurity oversight powers focusing on the Third and Eleventh Circuits, which could result in a state of affairs (unless Congress intervenes) in which no U.S. federal government agency can penalize a company simply for having lax cybersecurity unless it runs afoul of existing sector-specific statutory prohibitions.[108] Yet that does not mean that states could not act, as the California example demonstrates, along with new public-private partnerships as called for by applying the Ostrom Design Principles discussed further in Part IV.

B. ANALYZING THE NIST CSF

After being unable to convince Congress to pass comprehensive cybersecurity reform legislation, the Obama administration instead decided on an approach to nudge U.S. critical infrastructure toward greater cybersecurity due diligence.[109] The result was the first 2014 NIST Cybersecurity Framework (NIST CSF), which is critical since—even though it has been criticized as leading to a reactive stance[110]—it is promoting a baseline standard of care.[111] The NIST CSF is designed to "help organizations identify, implement, and improve cybersecurity practices, and create[] a common language for internal and external communication of cybersecurity issues."[112] The first NIST CSF was published in 2014,[113] and not too long thereafter it became established as an important data point for defining a "standard" for "due diligence."[114] Reminiscent of GDPR, the NIST CSF is also having a worldwide impact given active NIST collaborations with more than twenty nations.[115] Version 1.1 of the

108. *See, e.g.*, Adam Mazmanian, *Senate Bill Would Give FTC New Data Breach Authority*, FCW (Jan. 10, 2018), https://fcw.com/articles/2018/01/10/ftc-data-breach-mazmanian.aspx.

109. *See* NAT'L INST. OF STANDARDS & TECH., IMPROVING CRITICAL INFRASTRUCTURE CYBERSECURITY EXECUTIVE ORDER 13636: PRELIMINARY CYBERSECURITY FRAMEWORK 1 (2013), https://www.nist.gov/system/files/documents/itl/preliminary-cybersecurity-framework.pdf.

110. Taylor Armerding, *NIST's Finalized Cybersecurity Framework Receives Mixed Reviews*, CSO (Jan. 31, 2014, 7:00 AM), https://www.csoonline.com/article/2134338/nist-s-finalized-cybersecurity-framework-receives-mixed-reviews.html.

111. *See, e.g.*, Shackelford et al., *Bottoms Up*, *supra* note 82, at 308; Shackelford et al., *supra* note 66, at 27.

112. PWC, WHY YOU SHOULD ADOPT THE NIST FRAMEWORK 1 (2014), https://www.pwc.com/us/en/increasing-it-effectiveness/publications/assets/adopt-the-nist.pdf.

113. *See* NIST, FRAMEWORK FOR IMPROVING CRITICAL INFRASTRUCTURE CYBERSECURITY: IMPLEMENTATION OF EXECUTIVE ORDER 13636, at 26 (2015), http://www.nist.gov/cyberframework/upload/cybersecurity_framework_bsi_2015-04-08.pdf (noting that "[t]o allow for adoption, Framework version 2.0 is not planned for the near term").

114. John Verry, *Why the NIST Cybersecurity Framework Isn't Really Voluntary*, PIVOT POINT SEC., https://www.pivotpointsecurity.com/blog/nist-cybersecurity-framework/#:~:text=Some%20of%20the%20members%20in,they%20maintain%20are%20considered%20CI (May 25, 2017).

115. There is some evidence that this may already be happening, including with regards to the Federal Trade Commission's cybersecurity enforcement powers. *See, e.g.*, Brian Fung, *A Court Just Made It Easier for the Government to Sue Companies for Getting Hacked*, WASH. POST (Aug. 24, 2015, 2:03 PM),

NIST CSF was published in 2018,[116] which "boasts . . . improvements" in the areas of "authentication, supply chain cybersecurity, and vulnerability disclosure."[117] IoT has largely been left to the margins, which is a topic that NIST is gearing up to address in more detail.

C. CASE FOR A NIST IOT FRAMEWORK

NIST put out a draft IoT Cybersecurity Baseline and is gathering feedback on it as of this writing.[118] Such a Baseline could be supplemented by the 2019 NIST Privacy Framework, which takes a similar approach to the NIST CSF as a "tool developed in collaboration with stakeholders intended to help organizations identify and manage privacy risk to build innovative products and services while protecting individuals' privacy."[119] Legislation that is currently pending as of this writing, namely the IoT Cybersecurity Improvement Act of 2019 discussed next, would require NIST to finalize this process in collaboration with the Office of Management and Budget.

D. UNPACKING THE PROPOSED FEDERAL IOT LEGISLATION

Another path forward aside from bottom-up cybersecurity and data privacy frameworks facilitated by NIST is to rely more specifically on legislation to do what, thus far, standards have failed to deliver, building on recent developments of states like California. Senators Mark Warner, Cory Gardner, Ron Wyden, and Steve Daines introduced the Internet of Things Cybersecurity Act of 2017 with this aim in mind.[120] In essence, the legislation would leverage U.S. government procurement to only purchase products that: (1) "are patchable," (2) do not "contain known vulnerabilities," (3) "rely on standard protocols," and (4) they "don't contain hard-coded passwords."[121] Rather than a one-size-fits-all approach to regulating IoT, the authors provide a mechanism allowing industry to take up "equivalent, or more rigorous, device security requirements" than those envisioned in the Act.[122] Proponents of this effort include Bruce Schneier

---

https://www.washingtonpost.com/news/the-switch/wp/2015/08/24/a-court-just-made-it-easier-for-the-government-to-sue-companies-for-getting-hacked/.

116. *NIST Releases Version 1.1 of Its Popular Cybersecurity Framework*, NIST (Apr. 16, 2018), https://www.nist.gov/news-events/news/2018/04/nist-releases-version-11-its-popular-cybersecurity-framework.

117. Scott J. Shackelford, *Smart Factories, Dumb Policy? Managing Cybersecurity and Data Privacy Risks in the Industrial Internet of Things*, 21 MINN. J.L., SCI. & TECH. 1, 15 (2019).

118. *See NIST Releases Draft Security Feature Recommendations for IoT Devices*, NIST (Aug. 1, 2019), https://www.nist.gov/news-events/news/2019/08/nist-releases-draft-security-feature-recommendations-iot-devices.

119. *Privacy Framework*, NIST, https://www.nist.gov/privacy-framework (last visited Feb. 4, 2021).

120. MARK WARNER, CORY GARDNER, ROB WYDEN, & STEVE DAINES, INTERNET OF THINGS CYBERSECURITY IMPROVEMENT ACT OF 2017 FACT SHEET, https://www.warner.senate.gov/public/_cache/files/8/6/861d66b8-93bf-4c93-84d0-6bea67235047/8061BCEEBF4300EC702B4E894247D0E0.iot-cybesecurity-improvement-act---fact-sheet.pdf (last visited Feb. 4, 2021).

121. *Id.* at 1.

122. *Id.*

and Professor Jonathan Zittrain,[123] but it also has its critics.[124] Unfortunately, the bill died, due in large part to industry resistance,[125] leading one to consider alternatives. Indeed, other bills have also been addressed in Congress designed to improve IoT security, including the IoT Consumer TIPS Act of 2017, which is aimed at helping the FTC boost consumer cyber hygiene, as well as the SMART IoT Act, which would mandate that the U.S. Department of Commerce "conduct a study on the state of the industry."[126] In 2019, the IoT Cybersecurity Improvement Act of 2019 was introduced by Senator Mark Warner, which would require NIST and the OMB to establish new IoT cybersecurity guidelines for federal agencies.[127]

E. CIVIL SOCIETY

Rather than strict regulations, many industry groups prefer self-regulation "to [better] adapt to rapid technological progress."[128] In some circumstances, such efforts can be more cost effective than command and control-style regulation,[129] though it is not a panacea given that such efforts are voluntary and subject to market forces (for example, consumer demands), which is why communal self-governance is but one element of polycentric governance discussed in Part III.[130] One organization that is trying to create such a community is Consumer Reports through its *Digital Standard*, which was launched in 2017 and is designed "to measure the privacy and security of products, apps, and services . . . [to] put consumers in the driver's seat as the digital marketplace evolves."[131] The goal of the effort is to inform and empower consumers to make better decisions about the types of products and services

123. *Id.* at 2.

124. *See* Brian Krebs, *New Bill Seeks Basic IoT Security Standards*, KREBS ON SEC. (Aug. 1, 2017), https://krebsonsecurity.com/2017/08/new-bill-seeks-basic-iot-security-standards/.

125. *See S. 1691 (115th): Internet of Things (IoT) Cybersecurity Improvement Act of 2017*, GOVTRACK, https://www.govtrack.us/congress/bills/115/s1691 (last visited Feb. 4, 2021).

126. Robertson, *supra* note 107.

127. Internet of Things Cybersecurity Improvement Act of 2019, S. 734, 116th Cong. § 3 (2019).

128. MONROE E. PRICE & STEFAAN G. VERHULST, SELF-REGULATION AND THE INTERNET 21 (2005). According to Notre Dame Professor Don Howard, different online communities "have a complicated topology and geography, with overlap, hierarchy, varying degrees of mutual isolation and mutual interaction. There are also communities of corporations or corporate persons, gangs of thieves, and bands of angels doing charity on scales small and large." Don Howard, *Civic Virtue and Cybersecurity*, *in* THE NATURE OF PEACE AND THE MORALITY OF ARMED CONFLICT 181, 192 (Florian Demont-Biaggi ed., 2017). What is more, Professor Howard argues that these communities will each construct norms in their own ways, and at their own rates, but that this process has the potential to make positive progress toward addressing multifaceted issues such as enhancing cybersecurity. *Id.* at 193.

129. *See* PRICE & VERHULST, *supra* note 128, at 21–22.

130. Ostrom, *supra* note 65, at 2–3.

131. *Consumer Reports Launches Digital Standard to Safeguard Consumers' Security and Privacy in Complex Marketplace*, CONSUMER REPS. (Mar. 6, 2017), https://www.consumerreports.org/media-room/press-releases/2017/03/consumer_reports_launches_digital_standard_to_safeguard_consumers_security_and_privacy_in_complex_marketplace/.

based on privacy and security features, rewarding firms that make those attributes central components of their business models.[132]

As the *Digital Standard* is refined, it may well help shape global IoT governance.[133] Already, Consumer Reports is working with European colleagues to harmonize its *Digital Standard*, which could lead to further norm building efforts around cybersecurity due diligence in the IoT context as is discussed in Part IV.[134] However, obstacles remain in this context given the diverging regulatory stances of the United States and the EU when it comes to IoT governance, as is further explored in the analysis accompanying Table 1.[135]

III. E.U. CASE STUDY

The EU has long taken a more comprehensive approach to both cybersecurity and data privacy than the United States, which is now playing out in the IoT context.[136] For example, in late 2015 the European Commission launched Horizon 2020, which included goals for smart cities and IoT deployment,[137] with plans to secure the full range of IoT devices by extending product liability.[138] Indeed, even though there have not yet been sweeping changes to the IoT regulatory landscape, it is worth noting that France has extended the EU's Product Liability Directive to include IoT, making it the first—but likely not the last—EU Member State to take this step.[139] There has been a push to finalize the EU's ePrivacy Regulation, which is set to replace the 2002 ePrivacy Directive and will accompany and in some ways reinforce GDPR, but industry resistance has meant that as of this writing the Regulation remains in draft form.[140] The Netherlands' Radiocommunication Agency has also

132. *See Glow Pregnancy App Exposed Women to Privacy Threats, Consumer Reports Finds*, CONSUMER REPS., https://www.consumerreports.org/mobile-security-software/glow-pregnancy-app-exposed-women-to-privacy-threats/ (Sept. 17, 2020).

133. *See* Paul Hiebert, *Consumer Reports in the Age of the Amazon Review*, ATLANTIC (Apr. 13, 2016), https://www.theatlantic.com/business/archive/2016/04/consumer-reports-in-the-age-of-the-amazon-review/477108/ ("More than 120 employees, with an annual testing budget of approximately $25 million, evaluate some 3,000 products a year. The results of these impartial studies are then gathered, examined, and published, ad-free, in *Consumer Reports*."); Allen St. John, *Europe's GDPR Brings Data Portability to U.S. Consumers*, CONSUMER REPS. (May 25, 2018), https://www.consumerreports.org/privacy/gdpr-brings-data-portability-to-us-consumers/.

134. For a thorough accounting of international cybersecurity norms and how they overlap, see *International Cybersecurity Norms*, CARNEGIE ENDOWMENT INT'L PEACE, https://carnegieendowment.org/special projects/cybernorms/?lang=en (last visited Feb. 4, 2021).

135. *See infra* Part IV.

136. *See, e.g.*, Scott Shackelford, *Seeking a Safe Harbor in a Widening Sea*, CLS BLUE SKY BLOG (Nov. 4, 2015), http://clsbluesky.law.columbia.edu/2015/11/04/seeking-a-safe-harbor-in-a-widening-sea/.

137. EUR. COMM'N, HORIZON 2020 WORK PROGRAMME 2016–2017, at 90 (2015), https://ec.europa.eu/digital-single-market/sites/digital-agenda/files/discussions/h2020-wp1617-focus_en.pdf.

138. *Id.* at 90, 93.

139. *See* CONSTANCE E. BAGLEY, MANAGERS AND THE LEGAL ENVIRONMENT: STRATEGIES FOR BUSINESS 282 (9th ed. 2019); Lukasz Olejnik, *Highlights of the French Cybersecurity Strategy*, SEC., PRIV. & TECH INQUIRIES (Feb. 13, 2018), https://blog.lukaszolejnik.com/highlights-of-french-cybersecurity-strategy/.

140. *See* Kristof Van Quathem, *New Draft ePrivacy Regulation Released*, COVINGTON: INSIDE PRIVACY (Oct. 14, 2019), https://www.insideprivacy.com/international/european-union/new-draft-eprivacy-regulation-

supported expanding the European CE mark, which already applies to some twenty product groups such as appliance and toys, to include privacy and security benchmarks alongside safety, health, and environmental sustainability, but this proposal has similarly not yet been acted upon as of this writing.[141]

A. GDPR'S APPLICATION TO IOT SECURITY

One of the main ways that the EU will shape IoT governance is through GDPR, which is an expansive regulatory regime featuring a wide array of requirements on covered entities such as data portability and the right to be forgotten.[142] An important aspect is GDPR's push for covered entities to create codes of conduct as an affirmative defense against regulatory action, an example that Australia has followed with its new Code of Practice for the Manufacture of IoT Devices.[143] Yet these regulations were not drafted with IoT in mind, despite a 2017 finding by the European Union Agency for Network and Information Security (ENISA) "that there were no 'legal guidelines for IoT device and service trust.' Nor any 'level zero defined for the security and privacy of connected and smart devices.'"[144] Future European-level data protection regulation takes time—GDPR took more than four years to be adopted after first being proposed, meaning that relying on this same process to boost IoT security could prove problematic.[145] However, nations can go further than the EU as an organization. For example, the UK has also been active in developing cybersecurity standards, which is the illustrative example we turn to next. Such national case studies are important since the NIS Directive gives wide latitude to EU Member States to develop cybersecurity standards for critical infrastructure, and relatedly IoT.

B. NATIONAL CASE STUDY: UNITED KINGDOM & BREXIT

The UK has sought to secure critical infrastructure and in so doing help operationalize the NIS Directive through the development of IoT standards, a

released/. The nonprofit Internet Society also plans on publishing "concrete recommendations" to address IoT privacy and security risks in France. *Internet Society Advances IoT Security in France*, INTERNET SOC'Y (Jan. 8, 2019), https://www.internetsociety.org/news/press-releases/2019/internet-society-advances-iot-security-in-france/.

141. *See, e.g.*, *Dutch Regulator Calls for IoT Security Standards*, MOBILE EUR. (June 5, 2018), https://www.mobileeurope.co.uk/press-wire/13263-dutch-regulator-calls-for-iot-security-standards.

142. *See, e.g.*, INT'L ASS'N PRIV. PROS., TOP 10 OPERATIONAL RESPONSES TO THE GDPR 23–24 (2016), https://iapp.org/store/books/a191a0000027z5rAAA/.

143. *See* James Coker, *Australia Introduces Code of Practice for the Manufacture of IoT Devices*, INFOSECURITY MAG. (Sept. 4, 2020), https://www.infosecurity-magazine.com/news/australia-code-of-practice-iot/.

144. Scott Gordon, *Will We Get a GDPR for the IoT?*, INFOSEC ISLAND (Nov. 28, 2018), http://www.infosecisland.com/blogview/25140-Will-We-Get-a-GDPR-for-the-IoT.html.

145. *Id.*

process which began with the 2011 UK Cyber Security Strategy.[146] However, the 2011 Strategy did not specifically address IoT security.[147] As such, it was revised in 2014 to create the Cyber Essentials Certification Program,[148] which has the goal of "incentivis[ing] widespread adoption of basic security controls that will help to protect organisations against the commonest kind of Internet attacks."[149] Specifically, the Cyber Essentials Certification calls on businesses to follow the British government's Ten Steps to Cyber Security, which is reminiscent of the FTC's Guide for Business discussed in Part II.[150] The more recent 2016 UK National Cybersecurity Strategy moves forward on some of these issues, but only references IoT issues in passing.[151] Still, the Cyber Essentials Program has produced a following, and as a result has helped businesses across the country market cybersecurity as a competitive advantage, instead of merely a cost of doing business.[152] The British government has also made its Cyber Essentials Certification mandatory for all public-sector contractors handling PII.[153] Moreover, it has also announced plans to require applications geared for children to have built-in privacy protections.[154]

In short, Britain's Cyber Essentials effort is intended as supplementation of existing organizational approaches to risk management, but with plans for a mandatory IoT labeling scheme.[155] To that end, the IoT Security Foundation (IoTSF) has worked with IASME to create the IASME BASIC IoT Security Scheme, which aligns with and expands upon the Cyber Essentials Program. Beginning in April 2020, IASME has been chosen by the National Cyber Security Centre to be the sole Cyber Essentials Scheme Accreditation body for

146. UK CABINET OFF., THE UK CYBER SECURITY STRATEGY: PROTECTING AND PROMOTING THE UK IN A DIGITAL WORLD 27 (2011), https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/60961/uk-cyber-security-strategy-final.pdf.

147. *Id.*

148. UK CABINET OFF., THE UK CYBER SECURITY STRATEGY: REPORT ON PROGRESS AND FORWARD PLANS 7 (2014), https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/386093/The_UK_Cyber_Security_Strategy_Report_on_Progress_and_Forward_Plans_-_De___.pdf.

149. *Id.*

150. *10 Steps to Cyber Security*, NAT'L CYBER SEC. CTR., https://www.ncsc.gov.uk/collection/10-steps-to-cyber-security (last visited Feb. 4, 2021).

151. H.M. GOV'T, NATIONAL CYBER SECURITY STRATEGY 2016–2021, at 40 (2016), https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf.

152. *See About Cyber Essentials*, NAT'L CYBER SEC. CTR., https://www.cyberessentials.ncsc.gov.uk/getting-certified/ (last visited Feb. 4, 2021).

153. *See Policy Paper, 2010 to 2015 Government Policy: Cyber Security*, UK GOV'T, https://www.gov.uk/government/publications/2010-to-2015-government-policy-cyber-security/2010-to-2015-government-policy-cyber-security#appendix-7-working-with-industry-on-minimum-standards-and-principles (May 8, 2015).

154. *See* Fahmida Y. Rashid, *UK Says Children's Apps Must Have Built-In Privacy*, DECIPHER (Sept. 3, 2020), https://duo.com/decipher/uk-says-childrens-apps-must-have-built-in-privacy.

155. *See* Charles Towers-Clark, *UK to Introduce New Law for IoT Device Security*, FORBES (May 2, 2019, 11:34 AM), https://www.forbes.com/sites/charlestowersclark/2019/05/02/uk-to-introduce-new-law-for-iot-device-security/#4b0d8688579d.

the UK.[156] Relatedly, the UK has taken steps to clarify IoT labeling for consumers and manufacturers in an effort led by its Department for Digital, Culture, Media and Sport.[157] More recently, the UK government introduced legislation "to hold firms manufacturing and stocking Internet-connected devices to account to stop hackers threatening people's privacy and safety."[158] The legislation includes the prohibition of default passwords for IoT devices.[159] These developments place the UK as a unique success story of public-private collaboration in IoT security and highlights the different track it has taken from France, a division that may widen post-Brexit.[160]

It remains unclear, however, what impact Brexit will have on the UK's cybersecurity efforts generally, as well as IoT cybersecurity in particular. For example, the UK has taken the affirmative step of codifying GDPR into its domestic legislation through its Data Protection Act of 2018, which will presumably stay in effect regardless of the final Brexit settlement.[161] However, it is unclear whether or not the UK will continue to incorporate future updates or GDPR revisions into its domestic law, potentially placing British firms at a disadvantage to continental peers. If it voluntarily leaves, or is involuntarily thrown out, then it could place new barriers to British firms seeking to operate in the EU in the areas of creative content production, data protection, copyright, and e-commerce.[162] Related questions remain unanswered about Britain's post-Brexit participation in law enforcement collaborations like Europol, along with the impact on the EU if Britain limited its intelligence sharing with EU allies given its special position as a member of the Five Eyes.[163] IoT presents especially problematic issues given the broad ecosystem of devices and

156. *UK Government Cyber Essentials Scheme*, CST, https://www.cstl.com/CST/Cyber-Essentials/ (last visited Feb. 4, 2021).

157. *See Consultation on the Government's Regulatory Proposals Regarding Consumer Internet of Things (IoT) Security*, UK GOV'T, https://www.gov.uk/government/consultations/consultation-on-regulatory-proposals-on-consumer-iot-security/consultation-on-the-governments-regulatory-proposals-regarding-consumer-internet-of-things-iot-security (May 1, 2019).

158. Matt Warman, *Why the UK Is Banning Default Passwords in IoT Devices*, NS TECH (Jan. 27, 2020), https://tech.newstatesman.com/security/uk-banning-default-passwords.

159. *See id.*

160. *Cf.* Steve Ranger, *After Brexit, Europe Wants Cybersecurity Pact with UK*, ZDNET (Nov. 6, 2019), https://www.zdnet.com/article/after-brexit-europe-wants-cybersecurity-pact-with-uk/ (noting that the EU is keen to develop a cybersecurity intelligence sharing relationship with the UK post-Brexit).

161. *See GDPR and Brexit: How Will One Affect the Other?*, IT PRO (Jan. 9, 2020), https://www.itpro.co.uk/policy-legislation/31772/gdpr-and-brexit-how-will-one-affect-the-other.

162. *See* Ros Taylor, *Distress Signals: How Brexit Affects the Digital Single Market*, LSE BREXIT (Dec. 3, 2018), https://blogs.lse.ac.uk/brexit/2018/12/03/distress-signals-how-brexit-affects-the-digital-single-market/ ("This is because companies need an EU base (i.e. to be headquartered in the EU) to access service markets under Directives and Regulations which contain the country of origin (COO) principle (e.g. under AVMSD, SatCab, E-commerce and Copyright Directives).").

163. These worries come in two flavors: (1) operational impacts (that is, the nitty gritty of cyber deterrence and cybercrime investigation); and (2) policy impacts, namely the EU losing often the loudest voice for a more private-sector friendly, risk-management based approach to mitigating privacy and cybersecurity risks. This could push the EU to take an even harder line on protecting personal privacy, which might well be a boon for consumers, but could impact the types of innovative business that take root on the continent.

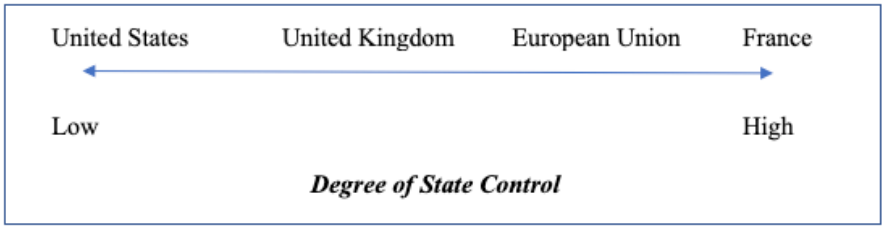
networks in question that often span national boundaries. If the UK is not part of broader EU efforts to develop IoT certifications and trustmarks, along with not employing updated versions of GDPR and the NIS Directive, it could further isolate British tech firms from finding new markets for their IoT products and services.

C. SUMMARY

The foregoing analysis highlights the disparity of approaches to IoT governance generally and security in particular that are being attempted in the United States and EU. The EU, for example, seems to be mirroring its approach to data privacy by moving in a direction of comprehensive regulation, particularly if more EU Member States follow France's lead in extending products liability to include IoT. The United States, on the other hand, is maintaining a largely voluntary, sector-specific approach to IoT security and privacy, though as leading states such as California enact new protections that might begin to change. The UK, perhaps in particular post-Brexit, seems to be positioning itself as a middle ground between these two bottom-up and top-down extremes, as exemplified in its Cyber Essentials Plus Certification public-private program and IoT security mandates. Still, such disparity makes it challenging for IoT firms with global ambitions to navigate between these competing regulatory schemes.

These results may be summarized in terms of an IoT governance spectrum, attempted in Figure 1 below, which is unpacked in Part IV. States with a relatively low degree of state involvement in IoT governance are positioned at the left side of this spectrum, with states—particularly those like France that now treat IoT as a component of products liability—on the right side.

Figure 1: IoT Governance Spectrum



Included within this governance spectrum is an array of different policy options that are being pursued in the transatlantic context, to say nothing of efforts underway across other cyber powers in Asia and beyond.[164] These

164. *See, e.g.*, JOHN CHEN, EMILY WALZ, BRIAN LAFFERTY, JOE MCREYNOLDS, KIERAN GREEN, JONATHAN RAY & JAMES MULVENON, CHINA'S INTERNET OF THINGS 45–46 (2018), https://www.uscc.gov/

include a spate of options described in Parts II and III ranging from safe harbors in Ohio to trustmarks in the EU, which are in turn summarized in Table 1.

Table 1: Approaches to IoT Governance

Type of Approach	Description	Example Jurisdiction
Safe Harbor	Incentivizing businesses to "develop and maintain a cybersecurity program that 'reasonably conforms' to an already existing, industry recognized cybersecurity framework" like the NIST CSF.[165]	Ohio
Reasonableness Standard	"[A]ny manufacturer of a device that connects 'directly or indirectly' to the Internet must equip it with 'reasonable' security features, designed to prevent unauthorized access, modification, or information disclosure."[166]	California
Dislosure Requirements	"Given the frequency, magnitude and cost of cybersecurity incidents, the Commission believes that it is critical that public companies take all required actions to inform investors about material cybersecurity risks and incidents in a timely fashion, including those companies that are subject to material cybersecurity risks but may not yet have been the target of a cyber-attack."[167]	SEC; state-level disclosure requirements
Data Privacy & Codes of Conduct	Incentivizes firms to develop industry codes of conduct to consider the wider risk of cyber threats to IoT ecosystems.	GDPR; Australia
IoT Trustmarks	Focusing on consumers by informing them of the risks posed by various IoT devices and services.	EU CE Marking
Products Liability	Treating breaches related to IoT products under a strict liability standard.	France

What mix of these approaches might make sense in a given context will be dependent upon the unique legal traditions and cultures of different jurisdictions. Thus, while there is certainly a place for benchmarks—such as the ability to update software for IoT devices—adequate room should also be made for bottom up experimentation and innovation, as we argue further in Part IV.

IV. POLICY IMPLICATIONS

This final Part reviews the policy implications revealed by the governance gaps highlighted above. First, we review what lessons can be learned from how the Internet itself evolved. Governance best practices are, in turn, analyzed and

sites/default/files/Research/SOSi_China's%20Internet%20of%20Things.pdf (noting the involvement of China in international IoT standards setting).

165. Mary Grob, *New Cybersecurity Law Offers Safe Harbor Against Tort Claims*, JD SUPRA (Nov. 26, 2018), https://www.jdsupra.com/legalnews/new-cybersecurity-law-offers-safe-91430/.

166. Robertson, *supra* note 107.

167. Commission Statement and Guidance on Public Company Cybersecurity Disclosures, 83 Fed. Reg. 8166, 8167 (Feb. 26, 2018) (to be codified at 17 C.F.R. pt. 229, 249).

applied to IoT. Second, we import these lessons as to the relative benefits of bottom-up and top-down approaches to managing an array of IoT governance challenges exemplified in Figure 1 to the field of cybersecurity due diligence in an effort to harden the emerging Internet of Things against nation-state attacks.

A. POLYCENTRIC INSTITUTIONAL ANALYSIS

The foregoing analysis paints a fragmented governance picture of the state of transatlantic IoT regulation. Indeed, given the pervasive types of devices, networks, and technologies that together comprise the Internet of Things, it is very unlikely that a unitary governance structure could or should be created to manage the myriad privacy and security threats faced within this context. Instead, as has been argued, a polycentric framework is useful in conceptualizing the state of IoT governance. This, in turn, helps to highlight gaps that may be taken advantage of by foreign national states and other adversaries. Table 2 represents an effort to distill the various regimes analyzed throughout the Article, which are mapped in turn onto the Ostrom Design Principles introduced above.

Table 2: Regime Effectiveness of IoT Governance Through the Lens of the Ostrom Design Principles[168]

Ostrom Design Principle	Applicability	Example Regulatory Regime	Explanation
Clearly Defined Boundaries	Contested	NIST CSF; FTC Guidelines	Defined boundaries are problematic given the extent to which various smart devices from automobiles to thermostats, and even toasters, interconnect to form ecosystems.
Fit to Local Conditions & Proportionality	Fostered	UK Cyber Essentials Plus Certificate; Digital Standard; Internet of Things Cybersecurity Act of 2017 (proposed)	The problem of proportionality is a frequent refrain in the cybersecurity context where few providers invest as much as they should in proactive cybersecurity measures because the full benefits of such investments are not realized by the firm.
Collective-Choice	Fostered	NIST CSF; Paris Call	This principle implies the importance of

168. This table is adapted from Forrest D. Fleischman, Natalie C. Ban, Louisa S. Evans, Graham Epstein, Gustavo Garcia-Lopez, & Sergio Villamayor-Thomas, *Governing Large-Scale Social-Ecological Systems: Lessons from Five Cases*, 8 INT'L J. COMMONS 428, 436 tbl.3 (2014).

Arrangements			engaged and proactive rulemaking by technical communities, the private sector, and the international community.
Monitoring	Fostered	Digital Standard; FTC; European Commission; Cybersecurity Tech Accord	According to Professor Ostrom, trust can typically only do so much to mitigate rule-breaking behavior. Eventually, some level of monitoring becomes important. In self-organized communities, typically monitors are chosen among the members to ensure "the conformance of others to local rules."[169]
Graduated Sanctions	Fostered	GDPR; 2018 California Law; FTC	Rule violations must not pass without notice or correction by the group.
Minimal Recognition of Rights to Organize	Present	GDPR, U.S. Constitution	This principle recognizes the importance of permitting stakeholders a say in organizing collective rules.
Nested Enterprises	Present	IETF; Consumer Reports; Information Sharing and Analysis Centers (ISACs)	Underscores the extent to which multilevel, multi-stakeholder governance structures are vital to instill governance best practices.

Although Table 2 does not represent a comprehensive analysis of the state of IoT governance and should only be considered among the first and certainly not the last word on how best to apply insights from the Ostrom Design Principles to this collective action problem, the analysis does reinforce several points that were raised throughout the paper. For example, it is clear that more needs to be done to clarify liability structures and, in so doing, simplify boundaries of responsibility within the Internet of Things. That is being done now in the EU, and to an extent in California as was discussed in Part II. Similarly, graduated sanctions need to be clarified, and enforced, across more jurisdictions. GDPR is a helpful step in this direction, as again is the 2018 California laws mentioned above, but they must be complemented by efforts

169. Ostrom, *supra* note 76, at 121.

from other G20 nations, as is discussed further below. Finally, public-private partnerships are needed to foster threat monitoring across these various networks and systems such as by taking advantage of successful nested entities like Internet Engineering Task Force (IETF).

In all, Table 2 underscores the extent to which top-down, global governance of IoT security is neither likely nor optimal given the extent to which polycentric structures are needed to define, monitor, and enforce best practices. This will result, and indeed already has resulted, in regulatory competition between Washington, Sacramento, Brussels, and even Beijing, among other players, but that is nothing new in the cybersecurity or data privacy context. The trick is, and will remain, to manage these competitions in ways that help promote good governance overall, similar to how Ostrom uncovered the benefits of small and medium-sized governance units over top-down approaches such as in the case of metropolitan policing.[170] Such insights not only have salience across domestic CPR contexts such as watersheds, but also online, as is explored next.

B. LOOKING BACK: APPLYING LESSONS FROM INTERNET GOVERNANCE TO IOT SECURITY

The Internet has succeeded rather well in spite of the fact that only the period of time that the Internet had any Internet-specific governance is before it became the Internet–the pre-Internet ARPANET (before 1983)—and for a few years thereafter. During this time, ARPANET, and the overlapping NSFNET, were paid for and operated under contract with the U.S. government.[171] But with the end of the government-run Internet backbone networks in the early 1990s and the rise of independent commercial Internet service providers came the end of an integrated governance structure. Instead, Internet service providers in the United States and elsewhere informally agreed to use the same set of technical standards and developed bilateral contracts between themselves.[172] Together, these agreements and complementary technical standards are what enabled the Internet to scale to the ubiquity that it enjoys today.

The Internet technical standards are a key part of the Internet's success and the standards did start with U.S. government action. A decade after the first nodes of the ARPANET were interconnected in 1969, ARPA chartered a committee, the Internet Configuration Control Board (ICCB) to "guide the technical evolution of the [Internet] protocol suite."[173] After several

170. *See, e.g.*, ELINOR OSTROM, ROGER B. PARKS, & GORDON P. WHITAKER, PATTERNS OF METROPOLITAN POLICING 2 (1978).

171. *See A Brief History of NSF and the Internet*, NAT'L SCI. FOUND. (Aug. 13, 2003), https://www.nsf.gov/news/news_summ.jsp?cntn_id=103050.

172. Memorandum from Vinton G. Cerf, Vice President of Corp. for Nat'l Rsch. Initiatives (May 1990), https://www.ietf.org/rfc/rfc1160.txt.

173. *Id.*

transformations the ICCB evolved into the IETF,[174] which is currently the primary technical standards body for the Internet.[175] The technical standards developed or maintained by the IETF are voluntary; the government does not mandate adherence to them but if an ISP or an equipment vendor does not support a core set of technical standards they would not be able to interoperate with the rest of the Internet. Proprietary standards for particular Internet applications do exist but their use is restricted to those systems that adopt the specific proprietary standards and even those systems must support the core set of technical standards in order for their communications to be transported over the Internet.

Unlike the major telecommunications standards organizations such as the International Telecommunications Union (ITU) and the European Telecommunications Standards Institute (ETSI), neither governments, nor their representatives, have any special role in the IETF standards development or approval. In addition, for more than two decades the IETF has been supported by meeting fees and the Internet Society and has not received direct support from any governments. Thus, the IETF is a fully independent international standards development organization, free from government influence, that creates standards that a rough consensus of IETF participants feel are technically sound.[176] As such, it mirrors the Ostrom design principles highlighting the value of nested, empowered governance through engaged communities working at various scales.

The IETF is currently working on IoT-related technical standards,[177] specifically including IoT security, but getting widespread adoption of the resulting standards will still be a challenge similar to the debate about how best to foster uptake of the NIST CSF. The IETF defines and maintains the standards for the technology that the Internet itself uses to transport information as well as the standards for the devices connecting to the Internet and the applications running on these devices and over the Internet. This technology includes security-enabling technology. As such, it plays an important role in Internet governance, which the United States and EU are working to augment.

Over the years there have been many attempts to formalize Internet governance, such as granting a greater governance role to the ITU.[178] But, to date, none of these efforts have succeeded, though there have been important milestones along the way such as the creation of the Internet Governance Forum

174. *Id.*; *see also About*, INTERNET ENG'G TASK FORCE, https://www.ietf.org/about/ (last visited Feb. 4, 2021).

175. Scott Bradner, *The Internet Engineering Task Force*, *in* OPEN SOURCES: VOICES FROM THE OPEN SOURCE REVOLUTION 47, 47 (Chris DiBona, Sam Ockman & Mark Stone eds., 1999).

176. *Id.*

177. Ari Keränen & Carsten Borman, *Internet of Things: Standards and Guidance from the IETF*, IETF J. (Apr. 17, 2016), https://www.ietfjournal.org/internet-of-things-standards-and-guidance-from-the-ietf/.

178. *See, e.g.*, Scott J. Shackelford, Enrique Oti, Jaclyn A. Kerr, Elaine Korzak, & Andreas Kuehn, *Back to the Future of Internet Governance?*, 16 GEO. J. INT'L AFF. 83, 84 (2015).

in 2006 and the U.S. Department of Commerce's decision not to renew its contract with the Internet Corporation for Assigned Names and Numbers (ICANN) in 2016.[179] However, taking the IETF as a model would argue that the United States voluntary security standards could be a successful path to security for the IoT, as opposed to the UK's Cyber Essentials Plus Certificate Program. But there is a significant difference between the Internet's voluntary technical standards and the voluntary security standards provided by NIST and others: a device that does not correctly implement the Internet technical standards will not be able to operate in the Internet, a strong forcing factor. On the other hand, a device that does not correctly implement security standards will interoperate, even though at a risk to the wider Internet ecosystem.[180] Thus, voluntary technical standards, on their own, will likely not be sufficient when it comes to IoT security given the market failures discussed in Part I.

C. LOOKING AHEAD: OPERATIONALIZING CYBERSECURITY DUE DILIGENCE IN THE IOT CONTEXT

At least two strategic paths forward can help firms, and the jurisdictions under which they operate, mitigate cyber risk in the IoT context. The first option is to further refine and operationalize the concept of cybersecurity due diligence, which is a general term used here in reference to enhancing the defense-in-depth utilizing multiple layers of protection of IoT devices along with the cyber hygiene of consumers. However, determining exactly what nations' due diligence obligations are to secure IoT devices and to prosecute or extradite cyber attackers is no simple matter.[181] A key aspect of this effort is effective information sharing; for example, government intelligence agencies cooperating with one another to detect such attacks and demonstrating a willingness to inform the targets. Without such information, the targets would often not even know if they were under attack, since few sophisticated attacks are detected,[182] and would not know that they needed to strengthen their defenses.

---

179. Elizabeth Weise, *U.S. Set to Hand Over Internet Address Book*, USA TODAY (Sept. 29, 2016, 8:52 PM), https://www.usatoday.com/story/tech/news/2016/09/29/icann-iana-internet-address-book-autonomous-department-of-commerce-ip-address-transition-internet-corporation-for-assigned-names-and-numbers/91281960/. For more on this history, see Scott J. Shackelford & Amanda N. Craig, *Beyond the New "Digital Divide": Analyzing the Evolving Role of National Governments in Internet Governance and Enhancing Cybersecurity*, 50 STAN. J. INT'L L. 119 (2014).

180. For more on this interconnection with broader conceptions of risk management particularly in the environmental context, see Scott J. Shackelford, *On Climate Change and Cyber Attacks: Leveraging Polycentric Governance to Mitigate Global Collective Action Problems*, 18 VAND. J. ENT. & TECH. L. 653 (2016).

181. *See* Mark Thompson, *Iranian Cyber Attack on New York Dam Shows the Future of War*, TIME (Mar. 24, 2016, 11:46 AM), http://time.com/4270728/iran-cyber-attack-dam-fbi/; Nicole Perlroth & David E. Sanger, *Cyberattacks Put Russian Fingers on the Switch at Power Plants, U.S. Says*, N.Y. TIMES (Mar. 15, 2018), https://www.nytimes.com/2018/03/15/us/politics/russia-cyberattacks.html; Andrea Peterson, *Sony Pictures Hack, Explained*, WASH. POST (Dec. 18, 2014, 1:15 PM), https://www.washingtonpost.com/news/the-switch/wp/2014/12/18/the-sony-pictures-hack-explained/?noredirect=on&utm_term=.20762a025643.

182. VERIZON, 2018 DATA BREACH INVESTIGATIONS REPORT 40 (11th ed. 2018), https://www.researchgate.net/publication/324455350_2018_Verizon_Data_Breach_Investigations_Report.

As we have seen, the United States and EU are taking different approaches toward IoT governance generally and increasing the responsibility for conducting cybersecurity due diligence by covered firms in particular. The United States has predominantly relied on a loose set of standards developed by NIST, IETF, and the World Wide Web Consortium (W3C), in collaboration with industry-specific groups, which are then (imperfectly and incompletely) enforced through FTC settlement orders. Yet recent developments—including California cybersecurity and privacy laws summarized above—will place new requirements on IoT manufacturers in a critical market that will likely cause many organizations to weigh whether it is worth designing specific products for California or making those standards the default. This process could be hastened by the growing uptake and popularity of the Consumer Reports *Digital Standard*, and mirrors the calculus that many, particularly in the United States, are having to undertake in considering how best to comply with GDPR.

In the EU generally, and the UK in particular, we are also seeing a growing interest in mandatory certification schemes to enhance IoT security against a range of cyber threats.[183] France might quicken this pace given its new approach to IoT product liability. As was shown, GDPR and the NIS Directive in particular are having an immediate impact on IoT manufacturers, which would only accelerate if the proposed French law shifting IoT liability is enacted (as with the pending IoT bills in Congress that were similarly summarized above). Eventually, such efforts could lead to greater harmonization, even a shared transatlantic approach to IoT security based around certain core fundamentals (such as banning hard-coded passwords, ensuring the ability to update devices, and enhancing consumer cyber hygiene) along with broader efforts to boost cybersecurity due diligence across the region.

Progress has also been made on defining the international norms for cybersecurity due diligence. The G7 Declaration on Responsible States Behavior in Cyberspace, for example, maintains that "States should not knowingly allow their territory to be used for internationally wrongful acts using ICTs."[184] The UN Group of Governmental Experts has reiterated this norm.[185] The *Tallinn Manual 2.0* Rule 6 maintains, "[a] State must exercise due diligence in not allowing its territory, or territory or cyber infrastructure under its governmental control, to be used for cyber operations that affect the rights of, and produce serious adverse consequences for, other States."[186] Other

183. *See, e.g.*, Gianmarco Baldini, Antonio Skarmeta, Elizabeta Fourneret, Richardo Niesse, Bruno Legeard, & Franck Le Gall, *Security Certification and Labelling in Internet of Things*, 2016 IEEE 3RD WORLD FORUM ON INTERNET OF THINGS (WF-IOT) 627, 628 (2016).

184. G7 DECLARATION ON RESPONSIBLE STATES BEHAVIOR IN CYBERSPACE 4 (2017), https://www.mofa.go.jp/files/000246367.pdf.

185. Rep. of the Grp. of Governmental Experts on Devs. in the Field of Info. and Telecomms. in the Context of Int'l Sec., ¶ 13, U.N. Doc. A/70/174 (July 22, 2015), https://digitallibrary.un.org/record/799853?ln=en.

186. TALLINN MANUAL 2.0 ON THE INTERNATIONAL LAW APPLICATION TO CYBER OPERATIONS 30 (Michael N. Schmitt ed., 2017).

stakeholders, including China, Kazakhstan, Kyrgyzstan, the Russian Federation, Tajikistan, and Uzbekistan have also maintained that nations should not "use information and communications technologies and information and communications networks to carry out activities which run counter to the task of maintaining international peace and security."[187] Eventually, such harmonization could lead to new international agreements on the scope and meaning of cybersecurity due diligence. However, such a day remains distant at present given the extent to which such statements paper over significant differences in what exactly constitutes due diligence especially in the context of censorship and cyber sovereignty.[188]

In general, then, there is a need for a polycentric approach to enhancing IoT cybersecurity to mitigate the risk of foreign nation-state cyber attacks on vulnerable devices and systems. At a foundational level, this includes securing the hardware and software supply chains on which these products are built.[189] It is similarly vital to leverage market forces to reward companies that take security and privacy seriously, such as through the *Digital Standard* and insurance industry. There is also a role for governmental regulations to help speed the uptake of cybersecurity due diligence best practices, as is happening now in both the EU and in California. Over time, such national and regional efforts will help to crystallize a cybersecurity due diligence norm, particularly as it pertains to the protection of critical infrastructure, which is being made increasingly "smart" and thus vulnerable to foreign nation-state cyber attacks. All of these governance levels are components of an effort to practice "deterrence by denial" as an alternative to the threat of offensive counterstrikes, though in reality both are being practiced.[190] Progress is being made at all of these governance levels, as has been discussed, including through the NIST CSF and EU's GDPR in particular. Yet further efforts are needed, as was made evident when the Information Systems Audit and Control Association (ISACA)[191] surveyed IT professionals in the UK and found that "75 percent of the security experts polled say they do not believe device manufacturers are implementing sufficient security measures in IoT devices, and a further 73 percent say existing security

187. Letter dated 9 Jan. 2015 from the Permanent Representatives of China, Kazakhstan, Kyrgyzstan, the Russian Federation, Tajikistan, and Uzbekistan to the United Nations addressed to the Secretary-General, U.N. Doc. A/69/723 (Jan. 13, 2015), https://documents-dds-ny.un.org/doc/UNDOC/GEN/N15/014/02/PDF/N1501402.pdf?OpenElement.

188. *See, e.g.*, Adam Segal, *Chinese Responses to the International Strategy for Cyberspace*, COUNCIL ON FOREIGN RELS. (May 23, 2011), http://blogs.cfr.org/asia/2011/05/23/chinese-responses-to-the-international-strategy-for-cyberspace/; Gerry Smith, *State Department Official Accuses Russia and China of Seeking Greater Internet Control*, HUFF. POST, http://www.huffingtonpost.com/2011/09/27/russia-china-internet-control_n_984223.html (Nov. 27, 2011).

189. *See* Shackelford et al., *supra* note 38, at 405.

190. *See* Scott J. Shackelford, Michael Sulmeyer, Amanda N. Craig Deckard, Ben Buchanan & Brian Micic, *From Russia with Love: Understanding the Russian Cyber Threat to U.S. Critical Infrastructure and What to Do About It*, 96 NEB. L. REV. 320, 335–38 (2017).

191. Previously known as Information Systems Audit and Control Association. *See About Us*, ISACA, http://www.isaca.org/about-isaca/Pages/default.aspx (last visited Feb. 4, 2021).

standards in the industry do not sufficiently address IoT *specific* security concerns."[192]

The international community has recognized the issues replete in the Internet of Everything. On November 12, 2018, French President Emmanuel Macron gave a speech at the Internet Governance Forum in Paris, announcing the Paris Call for Trust and Security in Cyberspace—a high-level multi-stakeholder statement of principles that did not necessarily break new ground in cyber norm building, but did crystallize several ongoing efforts including those mentioned above. In particular, the agreement calls for action to safeguard civilian infrastructure, promote Internet access, and make democracy harder to hack.[193] On the day it was announced, more than fifty nations (with the notable exception of the United States), along with "more than 130 companies and 90 universities and nongovernmental groups" signed the Paris Call.[194] Even though the United States, China, and Russia did not sign the accord, a number of cyber powers did, including the UK and France, and as such it is a prime example of the type of polycentric action needed to harden IoT devices.[195]

A number of trust-building steps should be taken on this journey. One final concrete idea that policymakers could consider is again pulled from the annals of Internet governance. In particular, "regional techs" were regular gatherings in which Internet architects got together to discuss operational issues and norms on the nascent Internet.[196] Over time, these gatherings morphed into the North American Network Operators Group (NANOG).[197] This might be a possible model for a technical-community-based group to develop operational standards and norms for the IoT governance and to supplement the existing ecosystem by providing a space for higher-level coordination. Such an iterative process, building on the success of initiatives like the NIST CSF, could prove helpful in clarifying questions of IoT governance and security, and ultimately encouraging more consumers—and requiring more manufacturers—to update their toasters and other IoT products.

192. *Existing Security Standards Do Not Sufficiently Address IoT*, HELP NET SEC. (Oct. 15, 2015) http://www.net-security.org/secworld.php?id=18981 (emphasis added).

193. *See* MINISTRY OF EUR. & FOREIGN AFFS., PARIS CALL FOR TRUST AND SECURITY IN CYBERSPACE (2018), https://www.diplomatie.gouv.fr/IMG/pdf/paris_call_text_-_en_cle06f918.pdf.

194. David E. Sanger, *U.S. Declines to Sign Declaration Discouraging Use of Cyberattacks*, N.Y. TIMES (Nov. 12, 2018), https://www.nytimes.com/2018/11/12/us/politics/us-cyberattacks-declaration.html; *Indiana University Among First to Endorse Paris Call for Trust and Security in Cyberspace*, NEWS AT IU (Nov. 12, 2018), https://news.iu.edu/stories/2018/11/iu/releases/12-paris-call-for-trust-and-security-in-cyberspace.html #:~:text=BLOOMINGTON%2C%20Ind.,at%20the%20Paris%20Peace%20Forum.

195. *See* MINISTRY OF EUR. & FOREIGN AFF., *supra* note 193.

196. *See Technical Community*, AM. REGISTRY FOR INTERNET NUMBERS, https://www.arin.net/about/relations/community/ (last visited Feb. 4, 2021).

197. *See What We Do*, NANOG, https://www.nanog.org/about/what-we-do/ (last visited Feb. 4, 2021).

CONCLUSION

As the IoT matures, so far it looks set to follow a similar route as the early days of Internet governance, though on an even larger scale, spanning myriad sectors and industries, in spite of the limitations of voluntary technical standards discussed above. Polycentric IoT regimes can help keep pace with these technological and regulatory changes.[198] This includes a mixture of standards—including a NIST IoT-specific effort—along with civil society efforts such as the *Digital Standard*, and the use of corporate governance structures, such as sustainability, and international norms, including due diligence. This all-of-the-above approach is vital to filling in governance gaps. As Professor Elinor Ostrom said, this is not a "keep it simple, stupid" response,[199] but a multifaceted one in keeping with the complexity of the crises in IoT governance.

198. *See* Adam Thierer, *Putting Privacy Concerns About the Internet of Things in Perspective*, INT'L ASSOC. PRIVACY PROS. (Feb. 3, 2014), https://iapp.org/news/a/putting-privacy-concerns-about-the-internet-of-things-in-perspective.

199. Jeffrey Weiss, *Elinor Ostrom and the Triumph of the Commons*, POL. DAILY (Oct. 14, 2009), http://www.politicsdaily.com/2009/10/14/elinor-ostrom-and-the-triumph-of-the-commons/. The Authors are grateful to Professors Fred Cate, David Fidler, and Anjanette Raymond among others for their comments, suggestions, and insights on developing portions of this argumentation.

***