WHEN TOASTERS ATTACK: A POLYCENTRIC APPROACH TO ENHANCING THE "SECURITY OF THINGS"

*Scott J. Shackelford J.D., Ph.D.**
*Anjanette Raymond***
*Danuvasin Charoen****
*Rakshana Balakrishnan*****
*Prakhar Dixit******
*Julianna Gjonaj*******
*Rachith Kavi********

There is a great deal of buzz surrounding the Internet of Things, which is the notion, simply put, that nearly everything not currently connected to the Internet, from gym shorts to streetlights, soon will be. The rise of "smart products" such as Internet-enabled refrigerators and self-driving cars holds the promise to revolutionize business and society. From 2013 to 2020, Microsoft has estimated that the number of Internet-enabled devices is expected to increase from 11 to 50 billion.[1] To substantiate the coming wave, Samsung recently announced that all of its products would be connected to the Internet by 2020.[2] Yet, there has been relatively little attention paid to how we should go about regulating this explosion in connected devices and still less

* Associate Professor of Business Law and Ethics, Indiana University Kelley School of Business; National Fellow, Stanford University Hoover Institution; Visiting Scholar, Stanford Law School; Senior Fellow, Center for Applied Cybersecurity Research.

** Assistant Professor of Business Law and Ethics, Indiana University, Kelley School of Business; Adjunct Assistant Professor of Law, Maurer School of Law, Indiana University; Visiting Fellow in International Commercial Law, Centre for Commercial Law Studies, Queen Mary, University of London.

*** Associate Professor, Associate Dean for Academic Affairs, NIDA Business School (Bangkok, Thailand).

**** Indiana University Kelley School of Business Information Systems Graduate Program.

***** Indiana University Kelley School of Business Information Systems Graduate Program.

****** J.D. 2016, Indiana University Maurer School of Law.

******* Indiana University Kelley School of Business Information Systems Graduate Program.

1. Karen Tillman, *How Many Internet Connections are in the World? Right. Now.*, CISCO BLOGS (July 29, 2013), http://blogs.cisco.com/news/cisco-connections-counter.

2. Jeff Parsons, *Every Samsung Product will be Connected to the Internet by 2020*, MIRROR (Jan. 6, 2015, 1:32 PM), http://www.mirror.co.uk/news/technology-science/technology/every-samsung-product-connected-internet-4927590.

about how cybersecurity should be enhanced across them. This Article analyzes possible approaches to regulating the Internet of Things to enhance cybersecurity with a particular focus on the literature of polycentric governance as a vehicle to help marry together bottom-up and top-down regulatory modalities.

TABLE OF CONTENTS

I. INTRODUCTION 417
II. UNPACKING THE "INTERNET OF THINGS" 421
A. *Birth and Growth of the IoT* 421
B. *Applying Lessons from Mobile Computing to the IoT* 424
C. *The Need to Address IoT Technical Debt* 426
D. *Comparative Case Studies Exposing Vulnerabilities in IoT Implementation* 429
1. *Retail Case Study* 432
a. RFID Tags 432
b. Powershelves 433
2. *Healthcare Case Study* 434
a. Remote Health-Monitoring Devices 435
b. IoT Devices in Clinical Care 435
c. Security and Privacy Considerations 436
III. REGULATING THE INTERNET OF THINGS 437
A. *Self-Regulation in the IoT* 437
B. *Federal Regulations Applicable to the IoT* 440
1. *Leveraging NIST Frameworks and the FTC to Boost the Security of Things* 442
2. *Federal Regulation Related to Retail IoT Activities* 446
3. *Federal Regulations Pertaining to IoT Healthcare Applications* 448
C. *State Approaches to Regulating the IoT* 450
1. *Progressive State Case Study: California* 450
2. *Common and Uncommon Approaches to Information Protection: Indiana and Florida* 451
3. *Summary* 452
D. *Applicable Comparative and International Law to Enhancing the Security of Things* 453
1. *European Union IoT Policies* 453
a. A Primer on the European Approach to Cybersecurity Regulation 455
b. European IoT Regulation 456
c. EU Big-Data Policy 458
d. The Internet of Everything EU-Policy Convergence 459
e. Other Notable IoT Regimes 459

E. Summary 464
IV. LEVERAGING POLYCENTRIC APPROACH TO ENHANCE THE SECURITY OF THINGS 464
A. An Introduction to Polycentric Governance and the IAD-SES Framework 464
1. Defined Boundaries 465
2. Proportionality 466
3. Collective-Choice Arrangements and Minimal Recognition of Rights 466
4. Monitoring 466
5. Graduated Sanctions and Dispute Resolution 467
6. IAD Summary 467
7. Enter the IAD-SES Framework 468
B. Implications for Managers and Policy-makers 468
V. CONCLUSION 474

> "We're now in a world where data is being collected all the time . . . We're bringing these devices into our homes, into what used to be private spheres, and the data that is being generated is increasingly much more sensitive. It's really in my mind fundamental that consumers continue to be in the driver's seat, that they have a say in their own information and how it's being used."
>
> —*FTC Commissioner Edith Ramirez*[3]

I. INTRODUCTION

On July 21, 2015, there was a car crash.[4] This in and of itself is not newsworthy given that there are, unfortunately, some 15,000 car accidents daily in the United States.[5] What made this episode different, though, was the fact that this crash was not the result of drunk driving or human error; rather, code was to blame.[6] Superstar hackers Charlie Miller and Chris Valasek took advantage of fundamental flaws, so-called "zero-day exploits,"[7] in the software running a Jeep Cherokee and used

3. T.C. Sottek, *The Internet of Things is Going to be a Legal Nightmare*, VERGE (Jan. 27, 2015), http://www.theverge.com/2015/1/27/7921025/will-self-regulation-be-a-huge-problem-for-privacy-in-the-internet-of.

4. *See* Andy Greenberg, *Hackers Remotely Kill a Jeep on the Highway – With Me in It*, WIRED (July 21, 2015, 6:00 AM), http://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway.

5. *See* NAT'L HIGHWAY TRAFFIC SAFETY ADMIN., 2015 MOTOR VEHICLE CRASHES: OVERVIEW (Aug. 2016), https://crashstats.nhtsa.dot.gov/Api/Public/ViewPublication/812318.

6. *See* Greenberg, *supra* note 4.

7. In a zero-day attack, a hacker creates an exploit before the vendor knows about the vulnerability, so the attack base is broader. There is little that users can do to slow down zero-days once they are unleashed, so an attacker "can wreak maximum havoc." Tony Bradley, *Zero Day Exploits: Holy Grail of the Malicious Hacker*, ABOUT TECH (Oct. 31, 2015), http://netsecurity.about.com/od/newsandeditorial1/a/aazeroday.htm. For more information on this and other types of cyber attacks,

these entry points to turn on the car's air conditioning, change the radio station while cranking the volume, turn on the windshield wipers, display a picture of themselves on the car's navigation screen, and eventually disable the car's transmission.[8] All of this was done from a laptop some ten miles away from the targeted Cherokee.[9] Though not the first time that a car had been hacked,[10] this episode did help raise the profile of what exactly is at stake with the rise of Internet-connected devices. Indeed, following this incident Chrysler announced a recall of 1.4 million affected vehicles, while Senators Ed Markey and Richard Blumenthal introduced an automotive security bill.[11] Unfortunately, though, given the vast and fragmented array of products and markets involved, promoting the "Security of Things" ("SoT") will take more than a single bill, or treaty for that matter. Rather, a new type of governance is needed to help foster "cyber peace" in an era increasingly defined by cyber insecurity.[12]

There is a great deal of buzz surrounding the Internet of Things ("IoT"), which is the notion, simply put, that nearly everything not currently connected to the Internet, from gym shorts to streetlights, soon will be.[13] The rise of "smart products" such as Internet-enabled refrigerators and self-driving cars holds the promise to revolutionize business and society. Applications are seemingly endless, and embrace an array of consumer products, including toasters.[14] Tesla's all-electric Model S sedan can now, for example, drive itself on the highway, as can Google's self-driving car.[15] In sum, from 2013 to 2020, Microsoft has estimated that

see SCOTT J. SHACKELFORD, MANAGING CYBER ATTACKS IN INTERNATIONAL LAW, BUSINESS, AND RELATIONS: IN SEARCH OF CYBER PEACE 111–50 (2014).

8. Greenberg, *supra* note 4. Miller, now a cybersecurity analyst at Twitter, was the first person to break into Apple's iPhone; he discovered a software flaw that would have allowed him to take control of every iPhone on the planet. He has won the prestigious Black Hat cybersecurity competition, among other awards, and worked for the NSA for five years. *See* Andy Greenberg, *Twitter Hires Elite Apple Hacker Charlie Miller To Beef Up Its Security Team*, FORBES (Sept. 14, 2012, 10:05 AM), http://www.forbes.com/sites/andygreenberg/2012/09/14/twitter-snags-elite-apple-hacker-charlie-miller-to-beef-up-its-security-team/; Andy Greenberg, *How to Hijack 'Every iPhone in the World'*, FORBES (July 28, 2009, 5:40 PM), http://www.forbes.com/2009/07/28/hackers-iphone-apple-technology-security-hackers.html. Christopher Valasek is "the Director of Security Intelligence at IOActive, an industry leader in comprehensive computer security services." *Christopher Valasek*, BLACKHAT USA 2014, http://www.rsaconference.com/speakers/chris-valasek (last visited Oct. 10, 2016).

9. *See* Greenberg, *supra* note 4.

10. *See id.*

11. *See id.*; Andy Greenberg, *Senate Bill Seeks Standards for Cars' Defenses from Hackers*, WIRED (July 21, 2015, 8:03 AM), http://www.wired.com/2015/07/senate-bill-seeks-standards-cars-defenses-hackers.

12. For more on cyber peace, see SHACKELFORD, *supra* note 7, at 111–50.

13. *See* Lawrence J. Trautman, *Cybersecurity: What About U.S. Policy?*, 2015 U. ILL. J.L. TECH. & POL'Y 341, 348 (2015); Daniel Burrus, *The Internet of Things is Far Bigger Than Anyone Realizes*, WIRED (Nov. 21, 2014), http://www.wired.com/2014/11/the-internet-of-things-bigger.

14. *See* Richard Baguley & Colin McDonald, *Appliance Science: The Internet of Toasters (and Other Things)*, CNET (Mar. 2, 2015, 11:26 AM), http://www.cnet.com/news/appliance-science-the-internet-of-toasters-and-other-things.

15. *See* David R. Baker, *How Self-Driving Cars Could Become Weapons of Terror*, S.F. CHRON. (Oct. 11, 2016, 6:51 AM), http://www.sfchronicle.com/business/article/How-self-driving-cars-could-become-weapons-of-9958541.php; Chris Welch, *Tesla's Model S Will Add Self-Driving 'Autopilot'*

the number of Internet-enabled devices is expected to increase from 11 to 50 billion, though estimates vary with Morgan Stanley predicting 75 billion such devices in existence by 2020.[16] To substantiate the coming wave, Samsung recently announced that *all* of its products would be connected to the Internet by 2020.[17] Regardless of the number, the end result looks to be a mind-boggling explosion in Internet connected stuff. Yet, the burning question is whether security can or will scale alongside this increasingly crowded field, or whether we will see a repeat of the late 1990s and early 2000s with products being rushed to market and attackers taking advantage of the resulting "technical debt."[18] So far, there has been relatively little attention paid to how we should go about regulating smart devices[19] and still less about how cybersecurity should be enhanced. This Article analyzes possible approaches to regulating the IoT economy to enhance cybersecurity with a particular focus on the literature of polycentric governance as a vehicle to help marry together bottom-up and top-down regulatory modalities.[20]

Polycentric governance is a multi-level, multi-purpose, multi-functional, and multi-sectoral model, championed by scholars including Nobel Laureate Elinor Ostrom and Professor Vincent Ostrom, which challenges orthodoxy by demonstrating the benefits of self-organization, networking regulations "at multiple scales,"[21] and examining the extent to which national and private control can, in some cases, coexist with communal management.[22] In many ways, this governance model—which has been applied to diverse collective-action problems ranging from

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.

16. *See* Tony Donava, *Morgan Stanley: 75 Billion Devices Will Be Connected To The Internet Of Things By 2020*, BUS. INSIDER (Oct. 2, 2013, 4:16 PM), http://www.businessinsider.com/75-billion-devices-will-be-connected-to-the-internet-by-2020-2013-10#ixzz3i4CApJsg.

17. *See* Rachel Metz, *CES 2015: The Internet of Just About Everything*, MIT TECH. REV. (Jan. 6, 2015), http://www.technologyreview.com/news/533941/ces-2015-the-internet-of-just-about-everything.

18. This is an industry term for the legacy costs of rolling out new products without first improving security. *See The Technical Debt Community*, ON TECH. DEBT, http://www.ontechnicaldebt.com/ (last visited Nov. 13, 2016)

19. *See* Scott R. Peppet, *Regulating the Internet of Things: First Steps Toward Managing Discrimination, Privacy, Security, and Consent*, 93 TEX. L. REV. 85, 94–95 (2015).

20. *See* 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 (2011) (defining polycentricity as "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").

21. *Id.* at 171–72; Elinor Ostrom, *Beyond Markets and States: Polycentric Governance of Complex Economic Systems*, 100 AM. ECON. REV. 641, 665 (2010).

22. Elinor Ostrom, *Polycentric Systems as One Approach for Solving Collective-Action Problems* 1 (Ind. Univ. Workshop in Political Theory and Policy Analysis, Working Paper No. 08–6, 2008) [hereinafter Ostrom, *Collective-Action*], http://dlc.dlib.indiana.edu/dlc/bitstream/handle/10535/4417/W08-6_Ostrom_DLC.pdf?sequence=1.

managing inner-city police precincts,[23] to adapting to climate change,[24] and even mitigating orbital debris[25]—is ideally situated to addressing dynamic (and oftentimes fragmented) IoT issues given the number of diverse actors and technologies in play. No governance system is perfect, and polycentric regulation has its disadvantages, such as concerns over gridlock and a lack of defined hierarchy.[26] We argue, however, that it could help move the debate regarding the Security of Things in a more productive direction as part of an overarching campaign to promote some measure of cyber peace.[27]

This Article is structured as follows. Part II unpacks the technical origins of IoT, surveying the suite of products that now comprise it and summarizing the vulnerabilities that plague many of these devices. Market leaders within the IoT field are also examined as case studies to help ascertain what role industry self-regulation can, and should, play in this context. Part III moves on to analyze applicable state, national, and international laws aimed at regulating the IoT, including the use of real-world examples and hypotheticals to identify governance gaps. Finally, Part IV investigates the utility of polycentric governance to conceptualize the SoT challenge, focusing, for the first time in the literature that we could identify, on applying the groundbreaking Institutional Analysis and Design-Social-Ecological Systems ("IAD-SES") Framework, along with related insights from the new governance literature before concluding with implications for managers and policymakers.[28]

23. *See generally* POLYCENTRICITY AND LOCAL PUBLIC ECONOMIES: READINGS FROM THE WORKSHOP IN POLITICAL THEORY AND POLICY ANALYSIS (Michael D. McGinnis ed., 1999) (collecting these studies).

24. *See* Elinor Ostrom, *A Polycentric Approach for Coping with Climate Change* 31–6 (World Bank, Pol'y Res. Working Paper No. 5095, 2009) [hereinafter Ostrom, *Climate Change*], http://www.iadb.org/intal/intalcdi/pe/2009/04268.pdf.

25. *See* Scott J. Shackelford, *Governing the Final Frontier: A Polycentric Approach to Managing Space Weaponization and Debris*, 51 AM. BUS. L.J. 429 (2014).

26. *See* Robert O. Keohane & David G. Victor, *The Regime Complex for Climate Change*17 (Harv. Kennedy Sch., Discussion Paper No. 10-33, 2010) http://belfercenter.ksg.harvard.edu/files/Keohane_Victor_Final_2.pdf.

27. *See* Henning Wegener, *Cyber Peace: A Concept of Cyber Peace*, *in* THE QUEST FOR CYBER PEACE 77, 77 (Int'l Telecomm. Union & World Fed'n of Sci. ed., 2011), http://www.itu.int/dms_pub/itu-s/opb/gen/S-GEN-WFS.01-1-2011-PDF-E.pdf. For a more general background on the application of polycentric governance to addressing cybersecurity, see Scott J. Shackelford & Andraz Kastelic, *A State-Centric Cyber Peace?: Analyzing the Role of National Cybersecurity Strategies in Enhancing Global Cybersecurity*, 18 N.Y.U. J. LEGIS. & PUBLIC POL'Y 895 (2016); Amanda N. Craig et al., *Proactive Cybersecurity: A Comparative Industry and Regulatory Analysis*, 52 AM. BUS. L.J. 721, 770–86 (2015); Scott J. Shackelford et al., *Using BITs to Protect Bytes: Promoting Cyber Peace by Safeguarding Trade Secrets Through Bilateral Investment Treaties*, 52 AM. BUS. L.J. 1, 52–73 (2015) [hereinafter Shackelford et al., *Using BITs*]; Scott J. Shackelford et al., *How Businesses Can Promote Cyber Peace*, 36 U. PA. J. INT'L L. 353 (2014) [hereinafter Shackelford et al., *Promote Cyber Peace*].

28. *See* Elinor Ostrom, *A General Framework for Analyzing Sustainability of Social-Ecological Systems*, 325 SCI. 419, 420 (2009). Other authors, however, have looked into security concerns within the IoT generally. *See* Anupam Chander & Uyen P. Le, *Data Nationalism*, 64 EMORY L.J. 677, 729 (2015); Kelsey Finch & Omar Tene, *Welcome to the Metropticon: Protecting Privacy in a Hyperconnected Town*, 41 FORDHAM URB. L.J. 1581, 1607 (2014); Dorothy J. Glancy, *Sharing the Road: Smart Transportation Infrastructure*, 41 FORDHAM URB. L.J. 1617, 1643 (2014); Woodrow Hartzog, *The Value of Modest Privacy Protections in a Hyper Social World*, 12 COLO. TECH. L.J. 333, 343 (2014); Paul

II. UNPACKING THE "INTERNET OF THINGS"

This Part begins by delving into the historic origins of the IoT, comparing and contrasting the development of smart devices with the early history of PCs and mobile phones. We next move onto the technical debt that is being amassed in the IoT landscape, followed by several industry case studies in the retail and healthcare contexts of firms that may be considered market leaders in addressing these pervasive vulnerabilities. This technical discussion sets the stage for the regulatory analysis in Part III and the need to address governance gaps to better keep pace with these rapidly evolving technologies in Part IV.

A. Birth and Growth of the IoT

The technology pioneer Kevin Ashton first used the expression "Internet of Things" as the title of a presentation for Proctor & Gamble in 1999.[29] He wanted to link the idea of the Radio Frequency Identification ("RFID") technology, which he had a hand in creating, to the Internet and thus attract the attention of senior executives.[30] Today, the term "IoT" enjoys wide usage in both technology circles as well as among policy-makers and in popular culture.[31] The idea of "intelligent" devices communicating with each other, however, dates back to long before the late 1990s, all the way to the emergence of ARPANET in late 1950s and 1960s, an undertaking that would eventually evolve into the Internet.[32] An IoT precursor came to be known as "pervasive computing" in the early 1970s.[33] By the 1990s, although more enterprises began to achieve more widespread Internet connectivity, slow speeds and poor network

---

de Hert & Vagelis Papakonstantinou, *Three Scenarios for International Governance of Data Privacy: Towards an International Data Privacy Organization, Preferably a UN Agency?*, 9 ISJLP 271, 301 (2013); Frank Pasquale & Tara Ragone, *Protecting Health Privacy in an Era of Big Data Processing and Cloud Computing*, 17 STAN. TECH. L. REV. 595, 620 n.149 (2014); Andrew Proia et al., *Consumer Cloud Robotics and the Fair Information Practice Principles: Recognizing the Challenges and Opportunities Ahead*, 16 MINN. J.L. SCI. & TECH. 145, 200 (2015); Adam Thierer, *The Internet of Things and Wearable Technology: Addressing Privacy and Security Concerns without Derailing Innovation*, 21 RICH. J.L. & TECH. 6, 6 (2015).

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

30. *Id.*

31. Jackie Fenn & Hung LeHong, *Hype Cycle for Emerging Technologies*, GARTNER (July 28, 2011), https://www.gartner.com/doc/1754719/hype-cycle-emerging-technologies.

32. Gil Press, *A Very Short History of the Internet of Things*, FORBES (June 18, 2014), http://www.forbes.com/sites/gilpress/2014/06/18/a-very-short-history-of-the-internet-of-things. ARPANET was created in 1958 in response to the Sputnik I launch. It first existed as a closed four-node network, connecting computers at the University of California, Los Angeles; Stanford University; the University of California, Santa Barbara; and the University of Utah. Eventually, it linked with other networks, adopted a common set of design protocols called Transmission Control Protocol and the Internet Protocol ("TCP/IP") that allowed diverse networks to talk to one another—giving rise to many security implications—and became *the* Internet. ANDREW W. MURRAY, THE REGULATION OF CYBERSPACE: CONTROL IN THE ONLINE ENVIRONMENT 63 (2006).

33. Fenn & LeHong, *supra* note 31.

architectures restricted the usage of interconnected machines.[34] In the early 2000s, applications were created that could provide access to information over the Internet in real time; however, these devices were still mainly interfaces that needed monitoring by a human presence.[35]

The true potential of IoT was realized only relatively recently when an explosion of devices operating dynamically—and based on insights gleaned from the processing of real-time information, and historical data with minimal human interaction came to fruition. Three main factors, in particular, have driven the explosive growth of the IoT since 2010.[36] First, the widespread availability of broadband Internet provided high-speed network connectivity that enabled devices to communicate with each other over a wireless network across large parts of the developed world.[37] Second, enhanced computational capabilities enabled the real-time analysis of large amounts of unstructured data.[38] Third, the decreasing cost of sensors allowed manufacturers to add small wireless chips to any device for a minor incremental cost.[39] The combination of these factors created the perfect environment for the proliferation of smart, interconnected devices, giving birth to the IoT.

Still, the evolution of IoT was slow, beginning in many cases as a collection of a relatively small number of devices such as sensors that could exchange information. For example, in the early 1980s, members of Carnegie-Mellon University placed micro-switches in a vending machine, permitting it to count the number of bottles present in the vending machine and determine their temperature.[40] IoT has now progressed a long way from smart vending machines, though, to include collections of quite dissimilar networks,[41] from residential buildings using integrated networks designed to control heating, ventilation and air control ("HVAC"), to smart thermostats that use predictive analytics to learn about user behavior patterns so as to create a customized heating sched-

34. Jim Chase, *The Evolution of the Internet of Things* TEXAS INSTRUMENTS, 1 (Sept. 2013), www.ti.com/lit/ml/swrb028/swrb028.pdf.

35. *Id.*

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

37. *Id.* Continuing digital divides persist between developed and developing nations with regards to Internet connectivity, meaning that the IoT has not evolved at the same rate globally. *See, e.g.*, David Bolton, *Developing Countries Will Drive the Growth of the Internet of Things*, ARC (Dec. 2, 2015), http://arc.applause.com/2015/12/02/internet-of-things-growth-developing-countries ("Developing countries have not really had the opportunity to interact or engage with the IoT thus far . . . .").

38. *See* Morgan, *supra* note 36.

39. *Id.*

40. *See* Press, *supra* note 32; *see also The Internet of Things: Groundbreaking Tech with Security Risks*, WELIVESEC. (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.").

41. DAVE EVANS, THE INTERNET OF THINGS: HOW THE NEXT EVOLUTION OF THE INTERNET IS CHANGING EVERYTHING, CISCO 4 (Apr. 2011), https://www.cisco.com/c/dam/en_us/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf.

ules.[42] As analytics and management capabilities improve, the HVAC system could be integrated with other networks such as telephone service, security, and lighting to create a remotely controllable smart home environment.[43] As the IoT matures, disparate smart residential and commercial networks will be able to communicate with one another, creating smart (and potentially more resilient) cities.[44] Such an ultimate, macro-level outcome resembles the early days of networking[45] when Cisco used multi-protocol routing to join dissimilar networks that eventually led to the creation a common networking standard called the Internet Protocol ("IP").[46] The IoT looks set to follow a similar route, albeit on a larger scale, spanning myriad sectors and industries.[47]

There is an increased focus on leveraging the advantages of IoT devices across economies. Table 1 illustrates some of the applications of IoT devices across various industries. As these devices mature, or so proponents argue, they will enable firms to achieve a higher degree of automation and efficiency in operations.

TABLE 1. CURRENT AND FUTURE APPLICATIONS OF IOT DEVICES ACROSS INDUSTRIES

Industry	Current Application	Future Scope
Retail	Supply chain operations; personalized marketing and customer service[48]	Real-time monitoring of in-store and fleet operations; consumer behavior prediction[49]
Healthcare	Diagnostic smartphones for patient vitals; pill bottle for prescription adherence[50]	Reducing device downtime using sensor data; telehealth services for elderly care[51]
Insurance	Existing technologies by the business are used to collect data for compliance[52]	Tailoring policies by using collected data to make business predictions[53]
Smart Home	Disparate networks like HVAC; lighting and security	Integration of all home-based networks to create a

42. Sharon Bohm, *How the "Internet of Things" is Changing the HVAC Industry*, RSI (April 12, 2016), https://www.refrigerationschool.com/blog/industry-news/how-the-internet-of-things-is-changing-the-hvac-industry.

43. *See id.*

44. *See id.*

45. EVANS, *supra* note 41, at 5.

46. *Id.*

47. *Id.*

48. Jonathan Gregory, *The Internet of Things: Revolutionizing the Retail Industry*, ACCENTURE STRATEGY, https://www.accenture.com/_acnmedia/Accenture/Conversion-Assets/DotCom/Documents/Global/PDF/Dualpub_14/Accenture-The-Internet-Of-Things.pdf.

49. *Id.*

50. Eric Topol, *The Future of Medicine Is in Your Smartphone*, WALL ST. J. (Jan. 9, 2015), http://www.wsj.com/articles/the-future-of-medicine-is-in-your-smartphone-1420828632.

51. *The Internet of Things for Health Care: A Comprehensive Survey*, IEEE ACCESS (June 1, 2015), http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=7113786.

52. Brett Jurgens, *How IoT Will Change Your Relationship with Insurance*, TECH. CRUNCH (Aug. 17, 2015), http://techcrunch.com/2015/08/17/how-iot-will-change-your-relationship-with-insurance/#.u6joyyv:3zq5.

53. *Id.*

	use smart devices like intelligent thermostats; smart meters for electricity and analytical security solutions[54]	single smart-home network which consists of all devices connected to each other seamlessly[55]
Automobile/Transport	Tracking traffic data; driver performance; environmental conditions; system alerts[56]	Connecting automated vehicles to other automated vehicles[57]

As Table 1 demonstrates, the IoT is not isolated to a particular sector or application, but rather is gaining ground across a broad range of products, services, and industries with the promise of revolutionizing business practices. In many ways, this evolution mirrors that which occurred in mobile phones with the more recent explosion in smartphone ownership.[58] Before moving on to the costs associated with the IoT—focusing on the cybersecurity aspects in particular—we analyze the growth of IoT in the context of other mobile computing platforms.

B. Applying Lessons from Mobile Computing to the IoT

The birth and evolution of IoT is linked with the story of other analogous mobile technologies. It is thus important to take a step back to better understand how mobile technologies and IoT influence one another. The advent of mobile technologies in the early 1990s essentially paved the way for IoT expansion that, as we will see, presaged many of the cybersecurity issues to follow.[59] Functionality and user operability have driven mobile-device growth among consumers.[60] As per a 2014 eMarketer study, more than 2.5 billion people across the globe will have smartphones by 2018.[61] An analysis of the Gartner report on worldwide device shipments in 2015 reveals that mobile computing devices (including mobile phones, tablets, and hybrids/clamshells) comprise nearly 90% of the total devices market, which is in turn expected to grow by approximately 5% in 2016.[62] The mushrooming mobile computing market has

54. Jeff John, *Smart Grid's Latest Cloud: Honeywell's Cloud-Connected Thermostats*, GREENTECH MEDIA (Nov. 3, 2011), http://www.greentechmedia.com/articles/read/smart-grids-latest-cloud-honeywells-cloud-connected-thermostats.

55. *Id.*

56. Jill Hayden, *Embracing Automated and Connected Vehicles*, INFRASTRUCTURE-INTELLIGENCE (May 27, 2015), http://www.infrastructure-intelligence.com/article/may-2015/embracing-automated-and-connected-vehicles.

57. *Id.*

58. *See* Mario Trujillo, *Pew: Rise of Smartphone Crowding Out Other Gadgets*, HILL (Oct. 29, 2015, 11:37 AM), http://thehill.com/policy/technology/258533-pew-smartphone-ownership-has-crowded-out-some-other-devices.

59. Pam Baker, *IoT and the Looming Mobile Tidal Wave*, INFO. WEEK (Apr. 28, 2015, 8:06 AM), http://www.informationweek.com/mobile/mobile-business/iot-and-the-looming-mobile-tidal-wave/a/d-id/1320182.

60. *Id.*

61. *2 Billion Consumers Worldwide to Get Smart(phones) by 2016*, eMARKETER (Dec. 11, 2014), http://www.emarketer.com/Article/2-Billion-Consumers-Worldwide-Smartphones-by-2016/1011694.

62. *Gartner Says Tablet Sales Continue to be Slow in 2015*, GARTNER (Jan. 5, 2015), http://www.gartner.com/newsroom/id/2954317.

led to a massive network of smart devices with extensive data gathering capabilities, all of which are powered by sensors in the back-end.[63] Devices like the iPhone created a demand for such sensor devices, both for basic operations as well as for advanced services such as geo-location monitoring, which in turn spurred the growth of the IoT.[64] Additionally, some mobile-networking technologies such as Bluetooth, WiFi, and 6LowPAN (Low Power Personal Area Network for IPv6) form the crux of networking protocols that enable IoT connectivity.[65]

One of the major differences between mobile technologies and IoT lies in the desired functionality for which these technologies were developed. To elaborate, mobile technologies were designed to enhance user interaction with portable devices, while IoT is designed primarily to enable devices to communicate with each other directly, without human intervention.[66] IoT and mobile computing have several functional differences as well. Innovators have been designing the IoT architecture such that it operates on a larger scale when compared to mobile computing architecture; IoT devices are being designed such that they are smarter with faster data transmission and processing capabilities, lower power consumption, smaller size, and advanced data-storage capabilities.[67] Moving forward, IoT will use these advanced functionalities and continue to leverage mobile computing technologies. For example, Philips Hue System already enables consumers to control household lighting by combining traditional lighting technology with advanced smart sensors controlled by mobile applications.[68]

From a security perspective for mobile computing, enterprises and organizations have been struggling to successfully deploy Bring-Your-Own-Device ("BYOD") programs, wherein users bring their personal devices to work.[69] While BYOD reduces the overall cost and can improve user productivity, cybersecurity concerns around remote network access and confidential-data protection have been some of the major draw-

63. Baker, s*upra* note 59.

64. *Id.*

65. *Id.* Created in 1981, IP version 4 (IPv4) allowed for more than four billion IP addresses, which early Internet architects thought would be sufficient for expansion. They were wrong. So, since 1992, engineers have been designing and attempting to implement a new system called IP version 6 ("IPv6"), which features a larger address space – on the order of billions of IP addresses for each person alive in 2013. Architects again imagine this scale to be inexhaustible. Time, and the related expansion of IoT devices, will tell if this is the case. *See, e.g.*, Kaushik Das, *Top 10 Features that Make IPv6 'Greater' than IPv4*, http://ipv6.com/articles/general/Top-10-Features-that-make-IPv6-greater-than-IPv4.htm (last visited Dec. 27, 2016).

66. *The Internet of Things: An Overview*, INTERNET SOC'Y (Oct. 2015), https://www.internetsociety.org/sites/default/files/ISOC-IoT-Overview-20151014_0.pdf.

67. *Id.*

68. Victor Brown, *"The Internet of Things" is the Next Big Market for Cloud*, CLOUDTECH (Jan. 8, 2014, 3:03 PM), http://www.cloudcomputing-news.net/news/2014/jan/08/the-internet-of-things-is-the-next-big-market-for-cloud-computing2.

69. *See* Dean Evans, *What is BYOD and Why is it Important?*, TECHRADAR~~D~~.PRO (Oct. 7, 2015), http://www.techradar.com/news/computing/what-is-byod-and-why-is-it-important--1175088.

backs.[70] Mobile Device Management ("MDM") solutions have been instrumental in helping to address these security gaps.[71] IoT, on the other hand, presents a whole new array of security threats with which enterprises need to cope.[72] For example, the U.S. National Fraud Intelligence Bureau conducted a survey in 2015 that found that approximately 70% of the more than 200,000 frauds recorded from 2013–2014 included a "cyber element, compared to approximately" 40% in 2009.[73] As such, "[i]t could be argued that if consumers cannot protect the devices that are already connected to the internet, perhaps we should not be adding more web-enabled devices to our homes and businesses."[74] Security (and relatedly helping to ensure against buggy code)[75] then becomes a focal point because IoT introduces a plethora of new devices and protocols resulting in massive data transmission and increased network traffic.[76] As is discussed in more detail next, Chief Information Security Officers ("CISOs") and equivalent leadership need to focus on improving access controls, network segmentation, and security analytics in order to better prepare their IT-security infrastructure to adapt to IoT advancements.[77]

C. The Need to Address IoT Technical Debt

Firms have racked up "technical debt," an industry term for the legacy costs of rolling out new products without first improving security,[78] in the IoT context, which is what occurred in both the mobile and PC contexts before. Like any debt, though, information is needed to best manage repayment. What makes IoT unique, and potentially more problematic than other mobile computing technologies, is the sheer scale and variability of devices and platforms in play. Indeed, while IoT offers promising value propositions with greater connectivity and functionality through ubiquitous networking, there are major challenges and issues that impact its implementation, some of which are summarized in Table 2.

70. *Id.*

71. *Everything You Need to Know About Mobile Device Management (MDM)*, CONTINUUM, https://www.continuum.net/msp-resources/mspedia/everything-you-need-to-know-about-mobile-device-management-mdm (last visited Dec. 27, 2016).

72. Jon Oltsik, *The Internet of Things: A CISO and Network Security Perspective*, ENTERPRISE STRATEGY GROUP 3 (Oct. 2014), https://www.cisco.com/web/strategy/docs/energy/network-security-perspective.pdf.

73. *See* Kim Walker, *The Legal Considerations of the Internet of Things*, COMPUTER WKLY. (July 2014), http://www.computerweekly.com/opinion/The-legal-considerations-of-the-internet-of-things.

74. *Id.*

75. *See* Violet Blue, *The Coming Smart-Thing Apocalypse*, ENGADGET: B@D P@SSW0RD (Oct. 29, 2015), http://www.engadget.com/2015/10/29/the-coming-smart-thing-apocalypse.

76. Oltsik, *supra* note 72, at 3.

77. *Id.*

78. *See, e.g.*, *Paying Down Your Technical Debt*, CODING HORROR (Feb. 27, 2009), http://blog.codinghorror.com/paying-down-your-technical-debt.

TABLE 2: CHALLENGES IMPACTING THE ADOPTION OF IOT

Challenge	Description
Security	Increasing the number of vulnerabilities that could be potentially exploited to conduct identity theft, steal information, penetrate networks, and even supplement physical attacks[79]
Privacy	Direct collection of sensitive-personally identifiable information and analysis of massive volume of granular data to make inferences about a person's behavior[80]
Data control and governance	Collection of a vast amount of real-time data overwhelming our capacity to protect it[81]
Standardization	Domination of proprietary protocols, interfaces and equipment designs, and lack of a standard, universally accepted architecture[82]

We discuss concerns with security and privacy in some detail here, as they pose arguably the most significant near-term challenges to the continued development and deployment of IoT systems; the related issues of governance and standards are unpacked further in Parts III and IV.[83] The dual issues of cybersecurity and privacy have been serious concerns throughout the rise of the Internet,[84] though IoT raises the stakes further. If someone's identity is hacked, that can hurt him or her financially.[85] If someone's autonomous car is hacked, the results may be even more damaging and more immediate.[86] Similarly, customized advertisements that are routinely seen while browsing highlight the implicit tradeoffs in the privacy bargain we have struck with leading tech firms.[87] As more dimensions of our behavior and aspects of our lives are tracked,

79. *Internet of Things: Privacy and Security in a Connected World*, FTC REP. (Jan., 2015), https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf; Peppet, *supra* note 19. *See also* Bernie Magkilat, *Critical Gov't Infrastructures Become Targets*, MANILA BULLETIN (Nov. 21, 2015), https://www.highbeam.com/doc/1G1-433284477.html (noting that "[a] the Internet of Things advances, Trend Micro said, smart devices or innovations that are used for public-facing technologies can be exploited, potentially causing virtual and physical destruction").

80. FTC REP., *supra* note 79.

81. *Safeguarding the Internet of Things: Being Secure, Vigilant, and Resilient in the Connected Age*, DELOITTE REV. 17 (July 27, 2015) [hereinafter "Safeguarding IoT"], http://dupress.com/articles/internet-of-things-data-security-and-privacy.

82. Rich Quinell, *10 Top Challenges Industrial IoT Must Overcome in 2015*, EE TIMES (Dec. 24, 2014), http://www.eetimes.com/document.asp?doc_id=1325067&page_number=2.

83. Michael Raynor, Author & Director, Deloitte, TM Forum Live Keynote: Strategy and the Internet of Things YOUTUBE (June 2, 2015), https://www.youtube.com/watch?v=YSwZyBEvOKU.

84. *See* SHACKELFORD, *supra* note 7, at 3–51.

85. Raynor, *supra* note 83.

86. *Id.*

87. *See* Casey Newton, *Tim Cook: Silicon Valley's Most Successful Companies are Selling You Out*, VERGE (June 2, 2015, 5:50 PM), http://www.theverge.com/2015/6/2/8714345/tim-cook-epic-award-privacy-security.

aggregated, and analyzed, it becomes increasingly the case that we are at risk of being manipulated without even being aware of it.[88]

When it comes to security, "IoT is like BYOD on steroids."[89] Before BYOD, any and every device was inside an organization's construct and was owned by its security team, *i.e.*, the devices could be controlled and hardened, and security policies could be pushed onto them as part of a contained ecosystem.[90] With BYOD, security teams cannot necessarily monitor or modify these devices that employees use to connect to internal networks and perform office tasks.[91] With IoT, this issue is exacerbated. IoT-enabled applications are within the core of a network while sensors and smart objects are outside the confines of the network, with data and intelligence being continuously transmitted between the secure and nonsecure environments.[92] To take one hypothetical, consider sensors deployed alongside a public road and used by traffic mapping applications. Those objects are in a public, insecure location, wherein a passing motorist could infiltrate the physical security or perform a hack while driving by to tap into any collected data.[93] There is some evidence that such attacks on increasingly smart cities are already happening.[94]

There is a vast amount of real-time data that is now being captured in scenarios like this by a growing number of smart devices we use every day. The scope of collected and communicated data now encompasses a wide swath of personally identifiable and sensitive information, including purchasing patterns, access codes, driving habits, and real-time location monitoring, to name a few.[95] Many technologies behind the IoT were not intended for secure communications, leaving networks and sensitive data vulnerable.[96] A new automobile, for example, can increasingly be thought of as a software package rather than a piece of hardware complete with numerous computational systems, GPS, diagnostic devices, infotainment systems, and connections to smart homes.[97] In fact, some types of auto-

88. Raynor, *supra* note 83.

89. Matt Hamblen, *Wearables Could Compromise Corporate Data*, COMPUTER WORLD (July 15, 2016, 3:00 AM), http://www.computerworld.com/article/3095852/security/wearables-could-compromise-corporate-data.html.

90. Raynor, *supra* note 83.

91. *Id.*

92. Oltsik, *supra* note 72, at 4.

93. Peter Sayer, *Connected Cars Gather Too Much Data About Their Drivers, Say Motorists Associations*, CIO (Nov. 26, 2015, 8:21 AM), http://www.cio.com/article/3009150/connected-cars-gather-too-much-data-about-their-drivers-say-motorists-associations.html.

94. *See, e.g.*, Lorenzo Franceschi-Bicchierai, *All the Ways to Hack a Smart City*, MOTHERBOARD (Apr. 8, 2015, 10:00 AM), http://motherboard.vice.com/read/all-the-ways-to-hack-a-smart-city; Dorothy J. Glancy, *Sharing the Road: Smart Transportation Infrastructure*, 41 FORDHAM URB. L.J. 1617, 1639–40 (2014); *see also infra* Part III.D.

95. *See* Shackelford et al., *Using BITs*, *supra* note 27, at 13–14.

96. *Id.* at 69–70.

97. Irfan Saif et al., *Safeguarding the Internet of Things*, 17 DELOITTE REV. 99, 112 (2015) [hereinafter *Safeguarding IoT*], https://dupress.deloitte.com/content/dam/dup-us-en/articles/internet-of-things-data-security-and-privacy/DUP1158_DR17_SafeguardingtheInternetofThings.pdf.

mobiles now have more lines of code running than Microsoft Windows.[98] One recent survey of automakers found that nearly *all* of the "cars currently on the market include wireless technologies that may be inadequately secure."[99] Even one vulnerable device leaves an entire ecosystem open to attack, causing significant and potentially lethal dangers to individuals and organizations. Hacking cars could, for example, provide access to smart homes and compromised industrial control systems, causing machinery or utilities to run dangerously out of control.[100] What makes IoT significantly vulnerable to exploits and attacks is that the IoT ecosystem connects multiple objects, machines, and people, not all of which can be securely controlled. Anything that is networked becomes a link in this increasingly long, insecure chain, which is only as strong as its weakest link.

D. Comparative Case Studies Exposing Vulnerabilities in IoT Implementation

In late 2013, the Washington, D.C. Department of Transportation overhauled its traffic management system by deploying a network of more than 1,300 wireless sensors to provide accurate data and insight for real-time congestion management, emergency response, and urban planning.[101] Less than a year later, Cesar Cerrudo, CTO at IOActive Labs, strolled the streets of the city and demonstrated how to hack into the deployed traffic-control systems from as far as two miles away, or even from a drone flying at more than 650 feet.[102] He exposed the vulnerabilities in the vendor's ("Sensys Networks") sensors, confirmed that the communications were not encrypted, and also showed that the sensors and repeaters could be controlled without any authentication.[103] This meant it was possible to fully compromise the sensors and feed traffic-control systems with fake data to manipulate traffic at will. It was also possible to create a firmware update worm that could further destabilize the system.[104] When contacted, the vendor replied that the devices have been designed intentionally without security built in to ease deployment.[105] At least 200,000 vulnerable sensors[106] from the same vendor have

98. *See* Robert N. Charette, *This Car Runs on Code*, IEEE SPECTRUM (Feb. 1, 2009), http://spectrum.ieee.org/transportation/systems/this-car-runs-on-code (noting that some automobile operating systems include more than 100 million lines of code). Windows XP had approximately 40 million lines of code. *See* GUY HART-DAVIS, MASTERING WINDOWS XP HOME EDITION 26 (2006).

99. Irfan Saif et al., *supra* note 97.

100. Tom Brewster, *There are Real and Present Dangers around the Internet of Things*, GUARDIAN (Mar. 20, 2014, 9:00 AM), http://www.theguardian.com/technology/2014/mar/20/internet-of-things-security-dangers.

101. Sensys Networks, *DDOT Implementation of Sensys Networks*, YOUTUBE (Sept. 18, 2013), https://www.youtube.com/watch?v=pb8nVvBxRgA#t=31.

102. IOActive, *Hacking Washington DC Traffic Control Systems*, YOUTUBE (July 29, 2014), https://www.youtube.com/watch?v=cKvbSb4uy0g#t=35.

103. *Id.*

104. *Id.*

105. *Id.*

been deployed worldwide, leaving an array of smart cities vulnerable to exploits. In April 2015, Mr. Cerrudo tested the same traffic sensors in San Francisco and found that the data communication was still not encrypted, even one year after his findings were published.[107]

To take another example, many IoT cameras have hardcoded credentials,[108] but numerous mobile applications do not encrypt traffic.[109] While this may seem less than significant, in fact the absence of encryption leaves the video stream open for anyone to view, meaning that somebody watching a video stream on his mobile phone connected to a public network allows others to sniff this information and watch the same video of the live traffic stream. The same happened when TRENDnet, a marketer of IoT cameras and baby monitors, "failed to use reasonable security to design and test its software, including a setting for the cameras' password requirement."[110] These devices also stored and transmitted login credentials in clear text, making them easily acquired and utilized by attackers.[111] Indeed, in early 2012, a hacker exploited these flaws and posted links to the live feeds of nearly 700 cameras.[112] Unfortunately, this vendor is not unique; as has been shown, many firms do not build in cybersecurity from the inception of new product lines, choosing too often instead to bolt it on after the fact.[113] IoT chipsets from as recently as two years ago did not have the capability to adhere to RSA or other cryptographic standards.[114] Today's IoT startups are still more focused on developing functionality at low costs rather than investing in more secure chips.[115] But this problem is not restricted to smaller companies. Even Nike Fuelband had a default pin on every device.[116] If anyone knew the default pin (which was not difficult to retrieve), one could connect to anybody's Fuelband. D-Link and Asus routers also have had backdoors

106. Cesar Cerrudo, *An Emerging US (and World) Threat: Cities Wide Open to Cyber Attacks*, IOACTIVE (2015), http://www.ioactive.com/pdfs/IOActive_HackingCitiesPaper_CesarCerrudo.pdf.

107. Nicole Perlroth, *Smart City Technology May Be Vulnerable to Hackers*, N.Y. TIMES: BITS (Apr. 21, 2015, 1:59 PM), http://bits.blogs.nytimes.com/2015/04/21/smart-city-technology-may-be-vulnerable-to-hackers.

108. Kelly Jackson Higgins, *4 Hurdles to Securing the Internet of Things*, INFO. WEEK: DARKREADING (Sept. 4, 2014, 6:10 PM), http://www.darkreading.com/informationweek-home/4-hurdles-to-securing-the-internet-of-things/d/d-id/1306978.

109. *Id.*

110. Press Release, Federal Trade Commission, Marketer of Internet-Connected Home Security Video Cameras Settles FTC Charges it Failed to Protect Consumers' Privacy (Sept. 4, 2013), https://www.ftc.gov/news-events/press-releases/2013/09/marketer-internet-connected-home-security-video-cameras-settles.

111. *Id.*

112. Dara Kerr, *FTC and TrendNet Settle Claim Over Hacked Security Cameras*, CNET (Sept. 4, 2013, 6:30 PM), http://www.cnet.com/news/ftc-and-trendnet-settle-claim-over-hacked-security-cameras.

113. Cerrudo, *supra* note 106.

114. Mark Stanislav, *Top 3 Security Issues in Consumer IoT and Industrial IoT*, IOT-INC. (Aug. 17, 2016), http://www.iot-inc.com/wp-content/uploads/2016/08/Video-16-Top-3-Security-Issues-in-Consumer-IoT-and-Industrial-IoT-Transcript.pdf.

115. *See, e.g.*, John Dixon, *Who Will Step Up to Secure the Internet of Things?*, TECH. CRUNCH (Oct. 2, 2015), http://techcrunch.com/2015/10/02/who-will-step-up-to-secure-the-internet-of-things.

116. Stanislav, *supra* note 114.

with default credentials that could not be changed.[117] The list goes on. In August 2014, researchers at the French technology institute Eurecom discovered thirty-eight vulnerabilities in the firmware across 123 products of IoT device manufacturers, which included poor encryption and backdoors that could allow unauthorized access.[118] Symantec analyzed fifty smart-home devices available in the market in 2015.[119] None of them enforced strong passwords or provided mutual authentication between the client and the server.[120] Two out of ten mobile applications "used to control the IoT devices did not use" the industry standard SSL to encrypt communications.[121] Most devices did not provide encrypted firmware updates.[122] The tested IoT platforms also contained other common vulnerabilities.[123]

These examples help illustrate the extent to which IoT is still in its nascent stage when it comes to security, with IoT devices having numerous security flaws—similar in many ways to the technical debt amassed by mobile providers and PC makers in the late 1990s and early 2000s.[124] As such, to narrow the analytical universe at issue, this Section uses comparative case studies to examine practices in both the retail and healthcare sectors, given that both of these arenas are among the fastest growing and largest consumer-facing markets within IoT, giving rise to numerous governance issues unpacked in Parts III and IV.[125] In particular, we focus on: 1) key IoT technologies, 2) the practices of industry leaders, 3) the impact of these trends on security and privacy, and 4) begin the discussion of how security, privacy experts, businesses, and policy-makers are reacting to these challenges that is continued in Parts III and IV.

117. *Id.*

118. Andrei Costin et al., *A Large-Scale Analysis of the Security of Embedded Firmwares*, USENIX (Aug. 20, 2014), https://www.usenix.org/system/files/conference/usenixsecurity14/sec14-paper-costin.pdf.

119. Mario Ballano Barcena & Candid Wueest, *Insecurity in the Internet of Things,* SYMANTEC (Mar. 12, 2015), https://www.symantec.com/content/en/us/enterprise/iot/b-insecurity-in-the-internet-of-things_21349619.pdf.

120. *Id.*

121. *Id.*

122. *Id.*

123. *Id.*

124. For more on this topic, see SHACKELFORD, *supra* note 7, at 111–50.

125. *See* Nathan Eddy, *IoT Market Will Grow 19 Percent in 2015, IDC Predicts*, INFO. WEEK (May 20, 2015, 10:10 AM), http://www.informationweek.com/it-life/iot-market-will-grow-19-percent-in-2015-idc-predicts/d/d-id/1320500 ("Thanks to growing use in the retail market, the one part of IoT is expected to grow from $6 billion in 2013 to $27.5 billion in 2018, representing a 35.7% five-year compound annual growth rate (CAGR)."); Patrick Oliver Graf, *The Biggest Cyber Threats Against Three At-Risk Verticals: Retail, Healthcare and Finance*, INFOSEC ISLAND (Dec. 3, 2014), http://infosecisland.com/blogview/24114-The-Biggest-Cyber-Threats-Against-Three-At-Risk-Verticals-Retail-Healthcare-and-Finance.html.

1. Retail Case Study

Industry adoption of IoT has been a driving force behind the rapid growth of the IoT ecosystem,[126] resulting not only in an array of new consumer products, but also the enhancement in business operational efficiency, supply chain monitoring, and growth of new business models.[127] Industries that will be leading in IoT investments from 2015 to 2019 are manufacturing, transportation, information technology, wholesale trade, healthcare, retail, finance, and utilities.[128] Total industry spending on IoT is estimated to reach $255 billion by 2019; industry leaders, however, have reservations about the cost of implementing IoT technologies, and the possibility of exposing their enterprise systems to the threat of cyber attacks.[129] As these statistics help make clear, IoT has redefined the way in which retail companies are operating, resulting in an increase in operational effectiveness and omni-channel experience.[130] In particular, retailers are using two technologies in the IoT context to help revolutionize their operations: RFID tags and Powershelves.

a. RFID Tags

One of the most popular uses of IoT in retail space is the use of RFID tags to manage products.[131] These tags help in the efficient identification and tracking of products, leading to robust inventory management.[132] As a pioneer in RFID implementation to improve supply chain and inventory, Walmart set the paradigm for other retail companies to follow.[133] Estimated benefits for Walmart arising from RFID implementation were $6.7 billion savings by reduction in labor costs, $600 million by reducing out-of-stock products, $300 million through efficient pallet tracking of one billion items, $575 million from theft/pilferage and administrative discrepancies, and $180 million by reducing inventory costs.[134]

126. John Greenough, *Forget Thermostats—IoT Adoption Will Be Driven by Companies Upgrading Factory Floors and Warehouses*, BUS. INSIDER (Nov. 20, 2014, 12:24 PM), http://www.businessinsider.com/iot-adoption-driven-by-companies-2014-11.

127. *Id.*

128. *Id.*

129. *Id.*

130. *See Cost Reduction in Retailing & Products Using RFID*, IDTECHEX (July 13, 2005) [hereinafter *Cost Reduction*], http://www.idtechex.com/research/articles/cost_reduction_in_retailing_and_products_using_rfid_00000205.asp.

131. Lalit Singla, *How Internet of Things (IOT) is Redefining the Future of Retail Industry*, NET SOLUTIONS INDIA (Aug. 3, 2015), http://www.netsolutionsindia.com/blog/how-internet-of-things-iot-is-redefining-the-future-of-retail-industry/#sthash.R8W4LhD4.dpuf.

132. *Id.*

133. Mark Roberti, *Wal-Mart Begins RFID Rollout*, RFID J. (Apr. 30, 2004), http://www.rfidjournal.com/articles/view?926.

134. *See Cost Reduction*, *supra* note 130.

In May 2015, Target, one of the leading U.S. retailers, also launched a RFID implementation program across its nearly 1,800 stores.[135] The initiative, through which Target will attach smart labels to product price tags, is aimed at improving inventory accuracy and maintaining items in stock to meet customer demand (specifically in cases of online orders with in-store pick up).[136] With online orders comprising nearly 15% of overall sales, Target has realized the immense potential that can be attained by reducing out of stock items through the use of RFIDs.[137] Implementation of IoT, however, including RFID tags, presents a set of challenges that retail companies and the general public are only beginning to consider.

One example of the downside of RFID tags is that retail companies can potentially combine data from RFID tags (which will be embedded in products purchased by the customer) with RFID tags in the customer's driving license/credit cards, to study customers without consent.[138] In 2010, use of RFID tags by Walmart came under heavy criticism by privacy experts and groups (such as Consumers Against Supermarket Privacy Invasion and Numbering) for RFID tracking that went beyond the store.[139] The onus is on the Walmart representative or customer to manually remove the tag after the product is purchased.[140] Since the tags are unlike typical electronic or ink tags, it may not be destroyed through washing or usage and might be active throughout the product life.[141] These potential vulnerabilities in RFID technology exposes the customer to privacy concerns erstwhile unheard of in retail shopping, thereby impacting shopper dynamics.

b. Powershelves

IoT is also revolutionizing the retail space by delivering experiential value to customers and business value to retailers. Whole Foods Market, one of the leading supermarket chains in U.S., has transformed their retail space through Powershelf (a product of Panasonic Corp.), which has been deployed in approximately forty outlet chains.[142] Through sensors

135. Claire Swedberg, *Target Announces Nationwide RFID Rollout*, RFID J. (May 20, 2015), http://www.rfidjournal.com/articles/view?13060.

136. *Target Rollout Expected To Be Retail's Largest By 2016,* RFID 24-7 (May 20, 2015), http://www.rfid24-7.com/2015/05/20/target-rollout-expected-to-be-retail%E2%80%99s-largest-by-2016.

137. *Id.*

138. Univ. Alliance, *RFID Technology Boosts Walmart's Supply Chain Management*, UNIV. OF S.F., http://www.usanfranonline.com/resources/supply-chain-management/rfid-technology-boosts-walmarts-supply-chain-management/#.WCpRv_krLic (last visited Dec. 27, 2016).

139. *Wal-Mart's Plan to Use Smart RFID Tags Sparks Privacy Concerns*, AOL: FINANCE (July 26, 2010, 3:45 PM), http://www.aol.com/article/2010/07/26/wal-marts-plan-to-use-smart-rfid-tags-sparking-privacy-concerns/19568512/?gen=1.

140. *Id.*

141. *Id.*

142. Claire Swedberg, *Panasonic Adds Bluetooth Beacons to Electronic Shelf Labels,* RFID J. (Feb. 4, 2015), http://www.rfidjournal.com/articles/view?12675.

attached to shelves, Whole Foods store operators automatically update prices from a centralized location which is then dynamically reflected on LCD screens on the shelves; they also receive notifications when shelves becomes empty and restocking is required.[143] In February 2015, Panasonic equipped Power shelves with Bluetooth Low Energy ("BLE") beacons so the sensors could send promotional push notifications to customers through mobile apps based on their proximity to the shelf.[144] Such technologies may transform the way customers interact with their surroundings in the retail space and enhance the retail experience.

Conversely, the growing concern among retailers is that beacons have not been scrutinized enough by federal regulatory authorities, and that implementing such a disruptive technology might be a potentially risky proposition.[145] Customers interact with the store through store apps (which are beacon enabled) downloaded on their mobile phones.[146] By downloading the app and agreeing to the terms and conditions, customers are not only sharing information, receiving promotional notifications, and using the app as a payment tool, but also are potentially allowing the technology to understand their shopping and lifestyle preferences through information stored on the phone.[147] With more than 70% of U.S. customers[148] using mobile phones while purchasing at retail outlets, this privacy threat could have far-reaching implications. It is imperative that retailers seek to proactively address the privacy and security risks posed by this technology prior to full-fledged deployment.[149]

2. Healthcare Case Study

In an industry with growing concerns over an acute shortage of primary-care physicians[150] and access to medical care in remote locations,[151] IoT holds the promise to deliver transformative benefits in the healthcare sector. As with retail, however, both privacy and security risks are replete in this increasingly crowded and dynamic marketplace. This case study briefly analyzes some of the benefits and implications of key

143. *Id.*
144. *Id.*
145. Calvin Berman, *Beacons at Retail – So What?*, SHEPPARD MULLIN: EYE ON PRIVACY (May 1, 2015), http://www.eyeonprivacy.com/2015/05/beacons-at-retail-so-what.
146. *Id.*
147. *Id.*
148. *See* Swedberg, *supra* note 142.
149. A point considered and being monitored by the FTC, see Benjamin Jensen, *FTC Hosts Workshop on Cross-Device Tracking*, JD SUPRA (Nov. 30, 2015) http://www.jdsupra.com/legalnews/ftc-hosts-workshop-on-cross-device-35788.
150. Christopher Cheney, *Physician Shortage to Quadruple Within Decade, AAMC Says*, HEALTH LEADERS MEDIA (Jan. 4, 2011), http://healthleadersmedia.com/page-1/PHY-258409/Physician-Shortage-to-Quadruple-Within-Decade-AAMC-Says.
151. Sam P.K. Collins, *What Life Without Medical Services Is Like for Residents in Rural Towns*, THINKPROGRESS (Nov. 25, 2014), http://thinkprogress.org/health/2014/11/25/3596516/documentary-rural-health-access.

IoT healthcare technologies focusing on remote health monitoring devices and the use of IoT devices in clinical care settings.

a. Remote Health-Monitoring Devices

Through IoT's innovative platform, medical care can be delivered to patients in remote and inaccessible locations.[152] Scanadu, a health electronics company, has helped revolutionize this space through their product Scanadu Scout, which collects, monitors, and analyzes vital health signs of the patients such as temperature, stress, systolic blood pressure, diastolic blood pressure, and respiratory rate in under ten seconds.[153] Walter De Brouwer, CEO of Scanadu, stated in an interview that he aims to shift the epicenter of healthcare to the comfort of the home by enabling smart phones to feed real-time health data to consumers and primary-care physicians alike.[154] Building on the Scanadu Scout, Scanada has also introduced Scana Flo, a urine analysis reader enabled through a smart phone (yet to be formally approved by the U.S. Food and Drug Administration ("FDA")), to measure various health parameters such as protein, glucose, nitrates, bilirubin, pH, and urobilinogen, and then relay such information to primary care physicians.[155] Such technologies have been enthusiastically adopted at an array of health centers across the nation. For example, Scanadu's Wi-Fi-based sensors have been a blessing in disguise for practitioners at The Oaks, an assisted care facility for senior citizens in South Carolina; immediate care can be provided by continuously monitoring patient movements and detecting anomalies.[156] Abbott Diabetes Care has also been innovating to provide a glucose monitoring system called FreeStyle Libre System, which continuously monitors glucose information through a sensor on the upper arm (for fourteen days) and transmits the information to the physician through a smart phone.[157]

b. IoT Devices in Clinical Care

IoT further provides advanced medical care in hospitals by using sensors to continuously monitor, collect, and transmit information to care givers, thereby enhancing the quality of healthcare rendered to pa-

152. David Niewolny, *How the Internet of Things Is Revolutionizing Healthcare*, FREESCALE (Oct. 2013), https://cache.freescale.com/files/corporate/doc/white_paper/IOTREVHEALCARWP.pdf.

153. *Scanadu Packs More Features into Scanadu Scout™; Unveils Design for ScanaFlo™*, SCANADU (May 22, 2013), https://www.scanadu.com/press/scanadu-packs-more-features-into-scanadu-scout-unveils-design-for-scanaflo.

154. *Internet of Things: Evolving Transactions into Relationships*, 1 PwC TECH. FORECAST 50 (2013) [hereinafter PWC TECH. FORECAST], http://www.pwc.com/us/en/technology-forecast/2013/issue1/assets/techforecast-2013-issue-1.pdf.

155. Press Release, Scanadu, Scanadu Packs More Features into Scanadu Scout(TM); Unveils Design for ScanaFlo(TM) (May 22, 2013), http://www.marketwatch.com/story/scanadu-packs-more-features-into-scanadu-scouttm-unveils-design-for-scanaflotm-2013-05-22.

156. *See* PWC TECH. FORECAST, *supra* note 154, at 19.

157. Spela Kosir, *Wearables in Healthcare*, WEARABLE TECH. (Apr. 15, 2015), https://www.wearable-technologies.com/2015/04/wearables-in-healthcare.

tients, while at the same time reducing costs for hospitals by eliminating the need for a professional to pay regular visits to monitor patient health.[158] For example, the Masimo Radical is a health monitor used in clinical environments to collect and transmit information on oxygen content, hemoglobin, respiration rate, pulse rate, etc., to doctors who can then get a more holistic, real-time update of patients' health.[159] Furthermore, IoT has also been entering clinical settings by allowing healthcare workers to track the progress of the patient at every stage in the recovery process, even after discharge. For instance, Proteus Digital health has developed indigestible sensors placed in pills that can monitor whether the patient has been taking the pills as scheduled.[160] After consumption, the pill emits a signal, which gets transmitted through the body tissue to a patch on the patient's skin that in turn transmits the information through smartphones to physicians.[161]

c. Security and Privacy Considerations

IoT innovations are expanding the horizons of healthcare monitoring and pushing the boundaries of excellence to provide affordable and accessible healthcare. Considering the regulatory landscape and privacy considerations, though, the healthcare industry is perhaps the most susceptible to the security implications of IoT.[162] Policy-makers and regulatory bodies are growing increasingly wary about the explosion of data through IoT, and are exploring ways to exercise regulatory oversight without stifling innovation in the healthcare context and beyond.[163] Some of these concerns are centered on ensuring that technology infrastructure is suitable to support IoT expansion, and that security mechanisms and privacy policies are in place to prevent intrusion from hackers and to govern usage of data collected from medical devices and sensors.[164] The National Institute of Standards and Technology ("NIST") has been implementing steps to secure the medical devices ecosystem, beginning with insulin pumps and expanding to other areas, as is discussed further in Parts III and IV.[165] For now, to a large extent, it is up to healthcare companies to self-govern and develop internal policies to tackle security and

158. Jaimy Ford, *Revolution Healthcare with "Internet of Things"*, AMERICA'S BACKBONE (Nov. 5, 2014), http://americasbackbone.com/evolve/revolution-healthcare-with-internet-of-things.

159. *Id.*

160. Laura Hamilton, *4 Ways The Internet of Things Is Transforming Healthcare*, FORBES: ELEVATE (Mar. 26, 2014, 5:57 PM), http://www.forbes.com/sites/85broads/2014/03/26/4-ways-the-internet-of-things-is-transforming-healthcare.

161. *Id.*

162. *How The IoT Will Impact Health Care Data Security,* PROTECTED TRUST (Aug. 14, 2015), https://protectedtrust.com/blog/how-the-iot-will-impact-health-care-data-security.

163. Daniel Castro, *Congressional Testimony for "The Internet of Things: Exploring the Next Technology Frontier*," DATA INNOVATION (Mar. 24, 2015), https://www.datainnovation.org/2015/03/congressional-testimony-for-the-internet-of-things-exploring-the-next-technology-frontier.

164. *Id.*

165. *Id.*

privacy concerns, setting the stage for the discussion of polycentric governance within these IoT contexts to follow.[166]

III. REGULATING THE INTERNET OF THINGS

As Professor Andrew Murray of the London School of Economics argues in the cybersecurity context, "[t]he market functions—but only so far!"[167] Governments also have a role to play to help the private sector meet cybersecurity and privacy challenges within the IoT, but what form should regulation take, and how can any adverse impact to innovation—especially in the retail and healthcare contexts—be minimized?[168] This Part reviews the regulatory landscape, taking note not only of applicable federal, state, and international law, but also other "regulatory modalities" popularized by Professors Lawrence Lessig and Yochai Benkler, including architecture and norms that "may be used individually or collectively" by policy-makers within the framework of polycentric governance.[169] Cyberspace is a dynamic, malleable environment, and, as such, an array of economic, legal, technical, and political forces should be brought to bear to enhance the Security of Things.

A. Self-Regulation in the IoT

There are many ways to conceptualize cyberspace regulation, but among them is the dynamic field of polycentric governance. This governance framework may be considered to be a multi-level, multi-purpose, multi-functional, and multi-sectoral model[170] that has been championed by numerous scholars, including Nobel Laureate Elinor Ostrom and Professor Vincent Ostrom, and challenges orthodoxy in part by demonstrating the benefits of self-organization and networking regulations "at mul-

166. *Id.*

167. MURRAY, *supra* note 32, at 200.

168. *See, e.g.*, Howard A. Schmidt, *The Administration Unveils its Cybersecurity Legislative Proposal*, WHITE HOUSE (May 12, 2011, 2:00 PM), https://www.whitehouse.gov/blog/2011/05/12/administration-unveils-its-cybersecurity-legislative-proposal (arguing for the need to strike a "critical balance between maintaining the government's role and providing industry with the capacity to innovatively tackle threats to national cybersecurity").

169. LAWRENCE LESSIG, THE FUTURE OF IDEAS: THE FATE OF THE COMMONS IN A CONNECTED WORLD 71 (2001). To help translate these insights into a regulatory framework for policymakers, Professor Yochai Benkler has introduced a simplified three-layer structure composed of: (1) the "physical infrastructure," including the fiber-optic cables and routers making up the physical aspect of cyberspace; (2) the "logical infrastructure," comprising necessary "software such as the TCP/IP protocol"; and (3) the "content layer," which includes data and, indirectly, users. Yochai Benkler, *From Consumers to Users: Shifting the Deeper Structures of Regulation Toward Sustainable Commons and User Access*, 52 FED. COMM. L.J. 561, 562 (2000).

170. 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. no.1, 2011, at 171–72 (Feb. 2011) (defining polycentricity as "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").

tiple scales."[171] It also posits that, due to the existence of free riders in a multipolar world, "a single governmental unit" is often incapable of managing "global collective action problems"[172] such as cyber-attacks. Instead, a polycentric approach recognizes that diverse organizations working at multiple levels can create different types of policies that can increase levels of cooperation and compliance, enhancing "flexibility across issues and adaptability over time."[173] Such an 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 norm cascade toward the Security of Things, as is explored further in Part IV.[174]

One important aspect of polycentric governance is self-regulation, which is vital to securing the pseudo, or "imperfect," commons of cyberspace.[175] The variety of such online communities abound—within the IoT context and more generally—as does their potential for successful self-regulation.[176] In some of these communities, such as eBay or Facebook—which Professor Murray describes as "Lockean" because users have given over some power to a central administrator—democratic governance can coexist with an established authority by, for instance, empowering users to police and report errant behavior.[177] This state of affairs may be compared to so-called Rousseauen communities in which power remains decentralized, which continues to be the current state of affairs in the IoT context.[178] Such groupings, however, are often ineffective, according to Professor Murray, because they are "simply too large and too diverse. . . ."[179] If, however, such communities could increase collaboration in the vein of Internet Engineering Task Force working groups, then power may not have to be centralized to the degree that it is in Lockean communities such as Facebook.[180] This may be accomplished through forming even smaller micro communities, potentially by making use of

171. Ostrom, *Collective-Action*, *supra* note 22, at 1.

172. Elinor Ostrom, *Climate Change*, *supra* note 24, at 35.

173. Robert O. Keohane & David G. Victor, *The Regime Complex for Climate Change* 9 PERSP. ON POL. 7, 15 (2011); *cf.* Julia Black, *Constructing and Contesting Legitimacy and Accountability in Polycentric Regulatory Regimes*, 2 REG. & GOVERNANCE 137, 157 (2008) (discussing the legitimacy of polycentric regimes, and arguing that "[a]ll regulatory regimes are polycentric to varying degrees").

174. *See* Martha Finnemore & Kathryn Sikkink, *International Norm Dynamics and Political Change*, 52 INT'L ORG. 887, 895–98 (1998).

175. JOSEPH S. NYE, JR., CYBER POWER 15 (2010).

176. MURRAY, *supra* note 32, at 148.

177. *Id.* at 163. John Locke was a seventeenth-century philosopher who is popularly known as the Father of Liberalism. *See* Jane Rutherford, *One Child, One Vote: Proxies for Parents*, 82 MINN. L. REV. 1463, 1469 (1998).

178. MURRAY, *supra* note 32, at 163. Jean-Jacques Rousseau was an eighteenth-century Genevan philosopher who argued that individuals are best protected from one another by forming a moral community of equals. *See* Katrin Froese, *Beyond Liberalism: The Moral Community of Rousseau's Social Contract*, 34 CAN. J. POL. SCI. 579, 581–82 (2001).

179. MURRAY, *supra* note 32, at 163.

180. For more on this topic, see Chapter 7 in SHACKELFORD, *supra* note 7.

social networking, as well as the so-called "cognitive surplus" of populations.[181] Polycentric theorists, including Professor Ostrom, have extolled the benefits of small, self-organized communities in the context of managing common resources,[182] and anthropological evidence confirms that groups of humans function more efficiently along certain metrics when they are kept relatively small in scale.[183] Micro-communities, however, like those focused on a single issue such as P2P file sharing, can ignore other interests, stakeholders, and the wider impact of their actions.[184] To overcome such apathy, these communities must have a defined stake in the outcome to effectuate good governance, which can be accomplished by educating users about the cyber threat and their power to help manage it, such as through Information Sharing and Analysis Organizations ("ISAOs") for different IoT market segments.[185]

The Internet is comprised of both types of communities, but a Lockean hybrid model favoring organic, bottom-up governance composed of small cybersecurity cohorts with a role for centralized coordination that can codify and enforce best practices, as well as protect against free riders, may be most appropriate to enhance IoT security.[186] Such self-regulation has the flexibility "to adapt to rapid technological progress"[187] arguably better and faster than black-letter law, which often

181. *See Digital Do-Gooders: Why Do We Help Strangers Online?*, BBC (Sept. 25, 2013), http://www.bbc.co.uk/news/magazine-24207047 (reporting that "educated people around the world have about a trillion hours of free time each year that could be contributed to collaborative projects, a phenomenon [Clay Shirky] calls 'cognitive surplus'"); *The New Politics of the Internet: Everything is Connected*, ECONOMIST (Jan. 5, 2013) [hereinafter *New Politics*], http://www.economist.com/news/briefing/21569041-can-internet-activism-turn-real-political-movement-everything-connected (discussing the ideas of Professor Kevin Werbach who has suggested that the Internet "lowers the barriers to organisation," potentially to the point that mailing lists could replace painstaking institution building).

182. *See, e.g.*, Elinor Ostrom et al., *Revisiting the Commons: Local Lessons, Global Challenges*, 284 SCI. 278, 278 (1999) (questioning policymakers' use of Garrett Hardin's theory of the "tragedy of the commons," in light of the empirical data showing self-organizing groups can communally manage common-pool resources).

183. *See, e.g.*, Gregory A. Johnson, *Organizational Structure and Scalar Stress*, *in* THEORY AND EXPLANATION IN ARCHEOLOGY 389, 392–94 (Colin Renfrew et al. eds., 1982).

184. *See* MURRAY, *supra* note 32, at 164 (explaining how members of micro-communities tend to focus only on what directly impacts their own activities); *cf. New Politics*, *supra* note 181 (discussing "the virtues of 'commons-based peer production' like that seen in open-source software communities, where volunteers write and debug code as a gift to the community at large").

185. Indeed, the retail sector has already established an ISAC in the wake of the 2014 Target data breach. *See* Retail Cyber Intelligence Ctr., *Retail-ISAC Launches Cyber Sharing Portal Supported by FS-ISAC*, PR NEWSWIRE (Mar. 24, 2015, 10:05 AM), http://www.prnewswire.com/news-releases/retail-isac-launches-cyber-sharing-portal-supported-by-fs-isac-300055086.html.

186. *See* MURRAY, *supra* note 32, at 164. The DHS Cybersecurity Awareness Month every October helps to highlight the important role played by bottom-up efforts to enhance cybersecurity. *See National Cyber Security Awareness Month*, DEP'T HOMELAND SEC., http://www.dhs.gov/national-cyber-security-awareness-month (last visited Dec. 27, 2016). Competitions rewarding communities that distinguish themselves in enhancing their cybersecurity along defined metrics, such as through grants, could also help build awareness and increase the potential for successful polycentric governance, especially when coupled with other hallmarks such as effective dispute resolution.

187. 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,

changes incrementally. It also has the potential to be more efficient and cost-effective than command and control-style regulation while instilling civic virtue,[188] though it is not a panacea, which is why communal self-governance is but one component of polycentric governance discussed further in Part IV.[189] Yet, as Professor Murray argues, "[i]n cyberspace the power to decide is, it seems, vested ultimately in the community. We have the power to control our destiny."[190] Indeed, the benefits of self-regulation are not absolute and depend on certain community characteristics, as is examined in the context of the IAD-SES Framework in Part IV, but various stakeholders, including the Federal Trade Commission ("FTC"), have seen the benefits of such a bottom-up approach—stating that it can be "'helpful' in encouraging companies to adopt privacy and security practices" as is explored further in the next Section before moving on to applicable state and international law.[191]

B. Federal Regulations Applicable to the IoT

Due to the breadth and complexity inherent in the field, federal cybersecurity law is largely ill-prepared to mitigate security problems arising in the IoT context.[192] As we will see, governance gaps are relatively common, only some of which are filled by relevant state and international law. Ultimately, the case is made that targeted IoT cybersecurity regulations should be adapted and improved to better keep pace with these changes,[193] particularly with regards to data regulations monitoring private firms and companies that transfer personally identifiable information.[194] This Subsection reviews the overarching federal regulations pertaining to the Security of Things, focusing in particular on the role played by the NIST Frameworks, before delving onto the federal regulations pertaining to the retail and healthcare sectors in particular.

The demand for a more comprehensive legal framework or regulatory system stems from the importance of protecting consumers while facilitating consumer confidence. There are a myriad of ways in which consumers can be harmed from security risks and breaches emanating from IoT devices, some of which were explored in Part II, particularly in the

and . . . on scales small and large." Don Howard, *Civic Virtue and Cybersecurity* 15 (Working Paper, 2014). 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 22.

188. *See* PRICE & VERHULST, *supra* note 187, at 21–22.

189. Ostrom, *Collective-Action*, *supra* note 22, at 2–3.

190. MURRAY, *supra* note 32, at 125.

191. Sottek, *supra* note 3.

192. *See* Peppet, *supra* note 19, at 133.

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

194. *See* Paul M. Schwartz & Edward J. Janger, *Notification of Data Security Breaches*, 105 MICH. L. REV. 913, 922 (2007).

retail and healthcare contexts. For example, granting access to personal information can lead to unfortunate impacts on personal livelihoods ranging from credit ratings to even personal safety.[195] Besides consumers personally suffering harm, the technology industry can also suffer setbacks if consumer confidence is undermined. Any perceived risk to privacy and security may result in the inability of technologies to reach their full potential in terms of both sophistication and adoption rates,[196] as has been seen in the economic impact of technology firms in the aftermath of the Snowden revelations.[197]

Furthermore, in addition to consumer confidence, consent is an issue that often arises in the evolving world of IoT.[198] In particular, debates have arisen about the applicability of the "Fair Information Practice Principles ("FIPPs"), which include such principles as notice, access choice, accuracy, data minimization, security, and accountability, and whether they should apply" to the IoT space.[199] Moreover, consent is connected to aspects of consumer-protection law relating to privacy-policy disclosures, which is another realm that is unprepared to address interlinked cybersecurity and privacy issues. For example, sensor devices are, in unique ways, capable of negatively impacting consumer welfare by leading (intentionally or not) to discrimination.[200] This is due to the fact that there is a public desire for new technologies, but consent is unlikely to provide reassurance to consumers.[201] Before delving into how the issue of cybersecurity, in particular, is dealt with in the case studies, we will review the role of federal agencies including NIST, which lies in the U.S. Department of Commerce, and the FTC in enhancing the Security of Things.[202]

195. Press Release, Fed. Trade Comm'n, FTC Report on Internet of Things Urges Cos. to Adopt Best Practices to Address Consumer Privacy and Sec. Risks (Jan. 27, 2015) [hereinafter FTC IoT Report], https://www.ftc.gov/news-events/press-releases/2015/01/ftc-report-internet-things-urges-companies-adopt-best-practices.

196. *See id.*

197. *See, e.g.*, Claire Cain Miller, *Revelations of N.S.A. Spying Cost U.S. Tech Companies*, N.Y. TIMES (Mar. 21, 2014), http://www.nytimes.com/2014/03/22/business/fallout-from-snowden-hurting-bottom-line-of-tech-companies.html?_r=0.

198. *See* FTC IoT Report, *supra* note 195.

199. *See id.* at ii.

200. Peppet, *supra* note 19, at 118.

201. *Id.* at 140.

202. The Federal Communications Commission ("FCC") also has an important role to play when it comes to enhancing cybersecurity in the IoT given "[t]he FCC's responsibility is to ensure the reliability and resiliency of the Nation's communications network and to promote public safety through communications." *Cyber Security and Network Reliability*, FED. COMM. COMM'N, https://www.fcc.gov/general/cyber-security-and-network-reliability (last visited Dec. 27, 2016). There is also evidence that the FCC is moving to more aggressively regulate privacy and cybersecurity matters, with the FCC collecting some $30 million in fines from telecom and cable companies after data breaches in 2015. Andrea Peterson & Brian Fung, *With This Hire, the FCC Could Soon Get Tougher on Privacy and Security*, WASH. POST (Nov. 24, 2015), https://www.washingtonpost.com/news/the-switch/wp/2015/11/24/with-this-hire-the-fcc-could-soon-get-tougher-on-privacy-and-security/ (noting that the FTC and FCC "have traditionally had different roles—with the FCC crafting rules for industry, while the FTC focuses more on law enforcement. But now they have shared territory").

1. Leveraging NIST Frameworks and the FTC to Boost the Security of Things

Given the lack of Congressional action on cybersecurity legislation, President Obama signaled, in his 2013 State of the Union address, his desire for the executive branch to partner with the privacy industry to develop a cybersecurity framework comprised partly of private-sector best practices that would help guide firms of all sizes, but particularly critical infrastructure operators.[203] The result was the 2014 NIST Framework, which is important since—even though its critics argue that it helps to solidify a reactive stance to the nation's cybersecurity challenges[204]—it is arguably spurring the development of a standard of cybersecurity due diligence in the United States.[205] In particular, the NIST Framework harmonizes industry best practices to provide, its proponents argue, a flexible and cost-effective approach to enhancing cybersecurity that assists owners and operators of critical infrastructure in assessing and managing cyber risk. Instead of the Framework supplanting an organizations existing security system, NIST intends for the Framework to provide support by helping organizations "identify, implement, and improve cybersecurity practices, and create a common language for internal and external communication of cybersecurity issues."[206] Although the NIST Framework has only been published for a relatively short time,[207] already some private-sector clients are receiving the advice that if their "cybersecurity practices were ever questioned during litigation or a regulatory investigation, the 'standard' for 'due diligence' was now the NIST Cybersecurity Framework."[208] Over time, the NIST Framework not only has the potential to shape a standard of care for domestic critical-infrastructure organizations, but could also help to harmonize global cybersecurity best practices for the private sector writ large, given active NIST collabora-

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

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

205. *See, e.g.*, Scott J. Shackelford et al., *Defining Cybersecurity Due Diligence Under International Law: Lessons from the Public and Private Sectors*, 17 CHI. J. INT'L L. 1 (2016); Scott J. Shackelford et al., *Toward a Global Standard of Cybersecurity Care?: Exploring the Implications of the 2014 NIST Cybersecurity Framework on Shaping Reasonable National and International Cybersecurity Practices*, 50 TEX. J. INT'L L.J. 303 (2015).

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

207. *See Framework for Improving Critical Infrastructure Cybersecurity*, NIST (Apr. 8, 2015), https://www.nist.gov/sites/default/files/documents/cyberframework/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").

208. John Verry, *Why the NIST Cybersecurity Framework Isn't Really Voluntary*, PIVOT POINT SECURITY (Feb. 25, 2014), http://www.pivotpointsecurity.com/risky-business/nist-cybersecurity-framework.

tions with more than twenty nations including the United Kingdom, Japan, Korea, Estonia, Israel, and Germany.[209]

Beyond the general 2014 NIST Framework, NIST also released another Framework focusing on the Internet of Things, entitled the "Framework for Cyber-Physical Systems" ("NIST IoT Framework"), in September 2015.[210] In essence, the NIST IoT Framework "is intended to serve as a common blueprint for the development of safe, secure, and interoperable systems as varied as smart energy grids, wearable devices, and connected cars."[211] Moreover, the Framework is also meant "to help manufacturers create new [Cyber-Physical Systems] that can work seamlessly with other such smart systems that bridge the physical and computational worlds."[212] Similar to the 2014 NIST Framework, the 2015 NIST IoT Framework was developed over an extended period of time with active participation from industry, academia, and the government and proposes to enhance the security of things by "providing a common set of considerations for the design of devices and a common language to allow designers to promote interactions between devices."[213] As with the 2014 NIST Framework, the 2015 NIST IoT Framework is a risk-based approach to managing cyber risk targeted at the IoT context. The goals of the NIST IoT Framework are to "derive a unifying framework that covers . . . the range of unique dimensions of CPS."[214] To aid in these goals, the NIST IoT Framework identifies CPS domains and analyzes and addresses cross-cutting concerns.[215]

Although both the 2014 NIST Framework and the 2015 NIST IoT Framework could help regulate IoT through the courts, such as by helping to define a standard for cybersecurity care in IoT negligence actions,[216] the FTC is also becoming increasingly active under Section 5 of the Federal Trade Commission Act, which regulates "unfair practices"[217]—using statutory authority to go after firms with particularly egre-

209. 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), 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.

210. Paul Otto & Brian Kennedy, *NIST Releases Draft Framework on the Internet of Things*, HOGAN LOVELLS CHRONICLE OF DATA PROTECTION (Sept. 25, 2015), http://www.hldataprotection.com/2015/09/articles/consumer-privacy/nist-releases-draft-framework-on-the-internet-of-things/.

211. *Id.*

212. Chad Boutin, *NIST Releases Draft Framework to Help 'Cyber Physical Systems' Developers*, NAT'L INST. STANDARDS & TECH. (Sept. 18, 2015), http://www.nist.gov/el/nist-releases-draft-framework-cyber-physical-systems-developers.cfm.

213. Otto & Kennedy, *supra* note 210.

214. *Preliminary Discussion Draft: Framework for Cyber-Physical Systems*, CYBER PHYSICAL SYS. PUB. WORKING GROUP (March 3, 2015, 5:27 PM), http://www.hldataprotection.com/files/2015/03/NIST-Cyber-physical-Framework-PRELIMINARY-DISCUSSION-DRAFT.pdf.

215. *Id.* at ix–x.

216. *See supra* text accompanying note 210.

217. Andrew Serwin, *The Federal Trade Commission and Privacy: Defining Enforcement and Encouraging the Adoption of Best Practices*, 48 SAN DIEGO L. REV. 809, 812 (2011).

gious privacy and security breaches.[218] One recent example is the settlement with Wyndham Hotel Group, where the FTC pursued "Wyndham Worldwide and three subsidiaries for allegedly storing data in plain text and other security failures that enabled hackers to access more than 600,000 payment card accounts in three data breaches in less than two years."[219] Under the terms of the settlement, Wyndham has to:

> [(1)] establish a comprehensive information security program designed to protect cardholder data – including payment card numbers, names and expiration dates . . . [(2)] conduct annual information security audits and maintain safeguards in connections to its franchisees' servers . . . [and (3)] certify . . . the 'untrusted' status of franchisee networks [as well as] the extent of compliance with a formal risk assessment process that will analyze the possible data security risks faced by the company.[220]

This order, which basically requires Wyndham to create a comprehensive cybersecurity policy that is regularly updated and vetted with third parties, has significant precedential value, but given how narrowly focused the order itself is, further FTC decisions are likely, especially given the Third Circuit ruling to uphold the FTC's authority to regulate the cybersecurity standards of commercial entities in August 2015.[221]

As was mentioned above,[222] the FTC believes that IoT-specific legislation would be premature at this time.[223] FTC Commissioner Ramirez, in particular, seems to support the idea that "Internet of Things" is a code word for self-regulation of things.[224] The FTC, however, has encouraged Congress to enact self-regulatory programs intended to incentivize the adoption of privacy and security best practices to protect against unauthorized access to both personal information and device functionality that are "strong, flexible, and technology-neutral," but that include well-defined rules for companies regarding how to provide choices to consumers about data collection and use practices.[225] The FTC also led a drive, in concert with the Obama Administration, to provide federal da-

218. Otto & Kennedy, *supra* note 210; *see also* Adam Steele, *An Emergency Room in Your Living Room: Privacy Concerns as Health Information Moves Outside of the Traditional Medical Provider Context*, 19 VA. J.L. & TECH. 388, 411 (2015) ("The FTC is the best-equipped federal agency to pursue such a strategy for a number of reasons. Most notably, the FTC is already focused on protecting consumer privacy and security in the modern 'Internet of Things'. . . .").

219. *See* Elinor Mills, *FTC Sues Wyndham Hotels Over Data Breaches*, CNET: NEWS (June 27, 2012, 2:46 AM), https://www.cnet.com/au/news/ftc-sues-wyndham-hotels-over-data-breaches.

220. Press Release, Fed. Trade Comm'n, Wyndham Settles FTC Charges it Unfairly Placed Consumers' Payment Card Information at Risk (Dec. 9, 2015) [hereinafter Wyndham Settles], https://www.ftc.gov/news-events/press-releases/2015/12/wyndham-settles-ftc-charges-it-unfairly-placed-consumers-payment.

221. *See* FTC. v. Wyndham Worldwide Corp., 799 F.3d 236 (3d Cir. 2015); *see also* FTC v. Wyndham Worldwide Corp., 10 F. Supp. 3d 602 (D.N.J. 2014).

222. *See infra* Part III.A.

223. FTC IoT Report, *supra* note 195.

224. Thiere, *supra* note 28, at 7–8.

225. *Internet of Things: Privacy & Security in a Connected World*, FTC STAFF REP. vii (Jan. 2015), https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf.

ta-breach notification regulations to consumers whose information has been compromised as part of a broader revision to the Consumer Privacy Bill of Rights.[226] It is worth noting that the FTC has been seeking more robust data protection laws since at least 2012, when Chairman Jon Leibowitz testified before Congress that the pace of self-regulation in the Internet industry needed to "accelerate."[227] Overall, the FTC recommendations have "three prongs: data security (companies should make devices physically secure from the outset), data minimization (companies should not collect more data than they need), and 'notice and choice' (let people choose what data to share, and tell them when you screw up)" to aid in this acceleration.[228]

During the 114th Congress, the Senate adopted an Internet of Things resolution which included language that:

(1) The United States should develop a strategy to incentivize the development of the Internet of Things in a way that maximizes the promise connected technologies hold to empower consumers, foster future economic growth, and improve our collective social well-being;

(2) The United States should prioritize accelerating the development and deployment of the Internet of Things in a way that recognizes its benefits, allows for future innovation, and responsibly protects against misuse;

(3) The United States should recognize the importance of consensus-based best practices and communication among stakeholders, with the understanding that businesses can play an important role in the future development of the Internet of Things;

(4) The United States Government should commit itself to using the Internet of Things to improve its efficiency and effectiveness and cut waste, fraud, and abuse whenever possible; and

(5) Using the Internet of Things, innovators in the United States should commit to improving the quality of life for future generations by developing safe, new technologies aimed at tackling the most challenging societal issues facing the world.[229]

This Senate resolution, vague on specifics as it may be, is a positive indicator as to Congress' view on both the central role of the private sector in developing and regulating the IoT and the degree of importance accorded this issue by policymakers (there were at least three separate

226. *Id.* at 20.

227. *FTC Issues Commission Report on Protecting Consumer Privacy*, FED. TRADE COMM'N (Mar. 26, 2012), https://www.ftc.gov/news-events/press-releases/2012/03/ftc-issues-final-commission-report-protecting-consumer-privacy.

228. Sottek, *supra* note 3.

229. A Resolution Expressing the Sense of the Senate about a Strategy for the Internet of Things to Promote Economic Growth and Consumer Empowerment, S. Res. 110, 114th Cong. (1st Sess. 2015).

hearings on IoT issues in Congress in 2015 alone).[230] Because IoT is rapidly advancing, though, existing regulations and laws are constantly in need of updating due to underlying changes in IoT technologies introduced in Part II in order to be effective in regulating IoT cybersecurity. This is particularly evident in the retail and healthcare contexts, which are discussed next before turning to state and international law.

2. *Federal Regulation Related to Retail IoT Activities*

While the 2014 NIST Framework and the 2015 NIST IoT Framework serve as a foundation to formulate effective IoT self-regulation, various sectors already boast specialized legal regimes applicable to IoT devices. One such area is retail, which is largely due to the central role played by consumers within the environment. Indeed, the cybersecurity and privacy of consumer information has long garnered regulatory attention, with the FTC serving as the primary federal agency on point.[231] The FTC's duties in this regard include enforcing: the FTC Act itself, the Fair Credit Reporting Act ("FCRA"), the health-breach notification provisions of the HI-TECH Act, and the Children's Online Privacy Protection Act.[232]

Within these very broad and encompassing regulations, Section 5(a) of the FTC Act, which pertains to the security and privacy practices of commercial entities, is the most relevant. Specifically, Section 5(a) of the FTC Act[233] "prohibits unfair or deceptive acts or practices affecting interstate or foreign commerce."[234] When considering the determination of violations of Section 5(a), the unfair and deceptive prongs are independently considered, thus each shall be considered in turn.

In determining the existence of a 'deceptive act' under FTC Section 5(a), the threshold is rather low, requiring merely any misrepresentation or omission of material fact.[235] The existence of a deceptive act is more

230. *See* RITA TEHAN, CYBERSECURITY: LEGISLATION, HEARINGS, AND EXECUTIVE BRANCH DOCUMENTS, CONG. RES. SERV. REP. R43317 12–21 (Oct. 21, 2016), https://www.fas.org/sgp/crs/misc/R43317.pdf.

231. Although state governments are exempt from FTC jurisdiction, private organizations must adhere to the FTC. *See* 15 U.S.C. § 45(a) (2012).

232. The FTC also works toward developing consumer education and business guidance; participation in multi-stakeholder efforts; and advocacy to other agencies at the federal, state, and local level. FTC IoT Report, *supra* note 195.

233. The FTC uses general authority under the FTC Act to penalize companies for security lapses. *See* Peppet, *supra* note 19, at 136.

234. *See* 15 U.S.C. § 45(a). Article 5, the relevant part of the FTC Act, stipulates that "unfair or deceptive acts or practices" in or affecting commerce are unlawful. MARKUS JAKOBSSON & ZULFIKAR RAMZAN, CRIMEWARE: UNDERSTANDING NEW ATTACKS AND DEFENSES 420 (2008).

235. *See, e.g.*, *A Brief Overview of the Federal Trade Commission's Investigative and Law Enforcement Authority*, FED. TRADE COMM'N (July 2008) [hereinafter *A Brief Overview*], https://www.ftc.gov/about-ftc/what-we-do/enforcement-authority ("The basic consumer protection statute enforced by the Commission is Section 5(a) of the FTC Act, which provides that 'unfair or deceptive acts or practices in or affecting commerce . . . are . . . declared unlawful.' (15 U.S.C. Sec. 45(a)(1)). Safe Web amended Sec. 5(a) 'unfair or deceptive acts or practices' to include such acts or practices involv-

likely to be substantiated in the case that the consumers had no means of knowing that there was a risk due to a misrepresentation or omission such that they could not reasonably avoid it. For example, as occurred in the previously discussed TRENDnet webcam case,[236] the FTC demonstrated that a company violated its own statement to consumers.[237]

The 'unfair' prong, however, demands the more detailed level of consideration of a three-factor test:

1. It causes or is likely to cause substantial injury to consumers;
2. The injury is not outweighed by countervailing benefits to consumers or competition; and,
3. It cannot be reasonably avoidable by consumers.[238]

As one can imagine from this test, gray areas cloud enforcement. For example, the FTC is required to demonstrate that a firm injured consumers in ways that violate public policy, such as when insufficient cybersecurity practices are present.[239] Demonstrating harm to consumers or showing that public policy has been violated is more feasible in highly regulated industries, such as healthcare, critical infrastructure, and finance, which must adhere to established federal statutory requirements. In less staunchly regulated industries, such as in many IoT areas like 'smart home devices,' the reach and authority of the FTC is less concrete.[240] Still, in such areas the FTC is playing an active role in the development of regulations, such as for governing companies that manufacture and develop interconnected devices. For example, the FTC recommends introducing cybersecurity measures in the beginning stages of a product design, rather than as an after-thought, conducting risk assessments, minimizing the amount and type of data collected, and vetting security measures ideally through third-party auditors before launching products.[241] In addition, and similar to the previously discussed NIST Framework, the FTC recommends that firms:

ing foreign commerce that cause or are likely to cause reasonably foreseeable injury within the United States or involve material conduct occurring within the United States.").

236. *In re* Trendnet, Inc., 2013 WL 4858250, No. 122-3090, at *4 (F.T.C. Sept. 3, 2013).

237. Peppet, *supra* note 19, at 137.

238. *See* 15 U.S.C. § 45(a); *see also*, *A Brief Overview*, *supra* note 235 ("'Unfair' practices are defined as those that 'cause[] or [are] likely to cause substantial injury to consumers which is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition' (15 U.S.C. Sec. 45(n)). In addition, the Commission enforces a variety of specific consumer protection statutes (e.g., the Equal Credit Opportunity Act, Truth-in-Lending Act, Fair Credit Reporting Act, the Cigarette Labeling Act, the Do-Not-Call Implementation Act of 2003, the Children's Online Privacy Protection Act, Fair and Accurate Credit Transactions Act of 2003, the Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003 and others)) that prohibit specifically-defined trade practices and generally specify that violations are to be treated as if they were 'unfair or deceptive" acts or practices under Section 5(a).'").

239. *See* Peppet, *supra* note 19, at 137.

240. *Id.* at 140.

241. *Cf.* Peppet, *supra* note 19.

1. Build security into devices at the outset, rather than as an afterthought in the design process;
2. Train employees about the importance of security and ensure that security is managed at an appropriate level in the organization;
3. Ensure that when outside service providers are hired, that those providers are capable of maintaining reasonable security and provide reasonable oversight of the providers;
4. When 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. Consider measures to keep unauthorized users from accessing a consumer's device, data, or personal information stored on the network;
6. Monitor connected devices throughout their expected life cycle and, where feasible, provide security patches to cover known risks.[242]

While these recommendations are in line with both the 2014 NIST Framework and the 2015 NIST IoT Framework, the FTC faces enforcement issues due to range, scope, cost, and compliance burdens, especially in the dynamic IoT context. Thus, the FTC—again similar to the approach used in designing the NIST Framework—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."[243] By taking such steps (such as limiting access of Powershelves platforms and building in security to RFID tags), the FTC is signaling that retailers can avoid being the subject of enforcement actions under Section 5(a).

3. Federal Regulations Pertaining to IoT Healthcare Applications

Even more than is the case with retail, healthcare remains among the most highly regulated sectors of the U.S. economy, including with regards to cybersecurity in the IoT context. For example, the Health Information Portability and Accountability Act ("HIPAA") has been modified and expanded to incorporate the Health Information Technology for Economic and Clinical Health ("HITECH") Act in 2009.[244] This is significant since the expansion provided for several critical changes rele-

242. FTC IoT Report, *supra* note 195.

243. *FTC Enters "Internet of Things" Arena With TRENDnet Proposed Settlement*, INFO. L. GP. (Sept. 9, 2013), http://www.infolawgroup.com/2013/09/articles/ftc/trendnet-settlement.

244. Modifications to the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules Under the Health Information Technology for Economic and Clinical Health Act and the Genetic Information Nondiscrimination Act; for other Modifications to the HIPAA Rules, see 45 C.F.R. 160 (2013).

vant to IoT. For instance, HIPAA's regulatory reach was extended to include business associates and subcontractors.[245] This revision gave more power to HIPAA, which, in turn, decreased regulatory ambiguity. Another change afforded more protection to consumers through increasingly stringent laws regulating the electronic transfer of personal health information ("PHI").[246] In fact, HIPAA was expanded to protect PHI outside the realm of traditional scope encompassing only covered entities. For example, this change to HIPAA allows for more regulation of the cloud, which has allowed healthcare operators to provide services remotely and is a technology central to many health IoT operators.[247] Since the scope of HIPAA is extended to business associates and subcontractors, fewer entities are inclined to employ inadequate protections due to the imposition of stricter and higher penalties.[248] Despite the HIPAA-HITECH expansion, however, significant governance gaps and areas for regulatory improvement still exist with regards to areas such as electronic health records, among other things. For instance, although HIPAA-HITECH has expanded its scope to encompass business associates and subcontractors in the cloud, there is ambiguity regarding any additional transmission of PHI within the cloud. Regulations and laws should be imposed to address the expanding area of the cloud that exceeds the scope of HIPAA. Although regulations are needed to address the transmission of PHI, enforcing any proposed laws will be difficult given already strained resources at the Health and Human Services Office for Civil Rights, which is responsible for enforcing HIPAA. Congress, however, may well approve the Office's increased budget request to enforce HIPAA's new Privacy, Security, and Breach Notification Rule Audit Program.[249]

Furthermore, it is essential that healthcare regulations be expanded because the evolving world of the IoT will surely incorporate PHI. Indeed, there are advantages to transferring PHI in exchange for a more convenient IoT world. For IoT to advance and succeed, however, not only does PHI need to be transferred, but regulations also need to exist to ensure consistency. Consistency will ensure consumer confidence, which, in turn, will allow the healthcare industry to successfully incorporate IoT.[250] States are also playing a role in this process, helping to address

245. *Id.*

246. *Id.*

247. *See A Guide to Healthcare IoT Possibilities and Obstacles*, TECH. TARGET, http://searchhealthit.techtarget.com/essentialguide/A-guide-to-healthcare-IoT-possibilities-and-obstacles (last visited Dec. 27, 2016).

248. Daniel Solove, *The HIPAA-HITECH Regulation, the Cloud, and Beyond*, TEACH PRIVACY (Jan. 26, 2013), https://www.teachprivacy.com/the-hipaa-hitech-regulation-the-cloud-and-beyond.

249. *See Overview of Budget Request*, OFF. CIV. RTS. 6 (2016), http://www.hhs.gov/sites/default/files/budget/office-of-civil-rights-budget-justification-2016.pdf.

250. John Glaser, *How the Internet of Things Will Affect Health Care*, HOSPITALS & HEALTH NETWORKS (Jun. 4, 2015), http://www.hhnmag.com/articles/3438-how-the-internet-of-things-will-affect-health-care.

governance gaps and form an increasingly important component of the burgeoning polycentric approach to enhancing the Security of Things.

C. State Approaches to Regulating the IoT

If the federal regulations do not apply to data-security breaches in the IoT context, then state law is referenced. As of 2016, forty-seven states had data-breach-notification laws.[251] These laws protect against the forfeiture of personal identifiable information ("PII"), including: first and last name, "social security number, driver's license number, or bank/credit card account information."[252] State laws protect against breach of PII or PHI, particularly in industries such as healthcare, where data portability is common.[253] Since many state data-breach-notification laws are narrow, though, "a security breach in theft of records" of consumers' "names and biometric or sensor data would" oftentimes fail to "trigger state data-breach requirements."[254] Some states and U.S. territories such as Arkansas, California, Missouri, and Puerto Rico, however, include "medical information" within PII.[255] Overall, though, most data-breach notification laws are not well equipped to alert the public on security problems emanating from IoT devices.[256] Moreover, a lack of consistency contributes to problems in state regulations, complicating the regulatory landscape for firms active across various state jurisdictions. For example, in regards to the healthcare industry, some states have their own definitions to apply to regulations, while others have adopted HIPAA definitions.[257]

1. Progressive State Case Study: California

Some states are advancing faster than others in adopting new laws and regulations to monitor privacy and security within the IoT. California is one of the leading states in maintaining more robust data protection and breach notification regulations regarding IoT, including in the retail and healthcare contexts. Laws pertaining to the protection of consumer data are outlined in the California Civil Code,[258] which includes regulations about the use and disclosure of PII and measures to take when a breach occurs. For instance, much like federal laws, in case of a breach of consumer personal information, action must be taken to notify

251. *Security Breach Notification Laws*, NAT'L CONF. ST. LEGISLATURES (Jan. 4, 2016), http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx.
252. *See id.*
253. Peppet, *supra* note 19, at 139.
254. *Id.*
255. *Id.* at 138.
256. *Id.* at 139–40.
257. *Id.* at 138–39.
258. CAL. CIV. CODE §§ 1798.29, 1798.80–.99 (West 2016).

consumers promptly through clear notice.[259] Furthermore, California's Civil Code includes laws more current and applicable to IoT-specific situations. For example, in January 2016, California expanded its definition of the term "personal information" to include "a person's name in combination with his or her Social Security number, driver's license or [state] identification card, credit or debit card number and password, or medical information."[260] In fact, some commentators suggest that "[w]hen the amendments take effect, 'personal information' will also include a person's name coupled with his or her health insurance information, and a username or email address in combination with a password or security question and answer that would permit access to an online account."[261] In addition, California law will now require "companies that share [such] information to not only take extra security precautions themselves when managing the information, but [also] to ensure that any entities they share information with also abide by strict security measures."[262] The implications of this "sharing information forward" regulation are expansive in that it creates "two broad categories of businesses—those which own, license, or maintain personal information about California . . . residents, and businesses which, pursuant to contract, disclose personal information about California . . . residents to unaffiliated third parties."[263] In practical effect, the regulation will require businesses to include within third-party information-sharing agreements "contractual provisions mandating implementation of reasonable security measures."[264] This could, for example, have the effect of further spreading both the 2014 NIST Framework and the 2015 NIST IoT Framework.

2. *Common and Uncommon Approaches to Information Protection: Indiana and Florida*

Like California, and similar to many states,[265] Indiana law imposes an *affirmative* obligation[266] on a "database owner"[267] to protect the PII[268]

259. CIV. § 1798.29(i)(5).

260. Dan Cook, *New Privacy Regs in CA, NV Tighten Security Measures*, BENEFITSPRO (Aug. 12, 2015), http://www.benefitspro.com/2015/08/12/new-privacy-regs-in-ca-nv-tighten-security-measure.

261. *See id.*

262. *Id.*

263. *Id.*

264. *Id.*

265. *See, e.g.*, Arkansas' Personal Information Protection Act, ARK. CODE ANN. § 4-110-104 (West 2016); Oregon Consumer Identity Theft Protection Act, OR. REV. STAT. § 646A.622 (2015); Texas Identity Theft Enforcement and Protection Act, TEX. BUS. & COM. CODE ANN. § 521.052 (2016) (using the term sensitive personal information).

266. *See* IND. CODE §§ 4-1-11-6, 24-4.9-3-1 (2016).

267. A "data base owner" is defined under the Indiana statute as a person or business that "person that owns or licenses computerized data that includes personal information" of an Indiana resident for commercial purposes." IND. CODE § 24-4.9-2-3.

268. "Personal information" is defined under the Indiana law as either: "(1) a Social Security number that is not encrypted or redacted, or (2) an individual's first and last names, or first initial and

of residents collected or maintained by the database owner. The Indiana State Data Breach Notification Law mandates that a database owner "shall implement and maintain *reasonable procedures*, including taking any appropriate corrective action, to protect and safeguard from unlawful use or disclosure any personal information of Indiana residents collected or maintained by the data base owner."[269] Also, in a similar vein to many states,[270] the Indiana Attorney General may bring an action against any business that violates the Indiana statute to obtain civil penalties and obtain an injunction against future violations.[271] Unlike Indiana, in 2014 Florida became one of the first states to amend its breach-notification laws to shorten the deadline for breach notification, to create a requirement for businesses to provide copies of forensic reports and "policies regarding breaches" to the Florida Attorney General upon request, and to expand the definition of "personal information" to include online account credentials.[272]

3. Summary

These state practices demonstrate the varying approaches being adopted by states as they seek to safeguard consumer security and privacy in the IoT context, but also more broadly. Such bottom-up experimentation is part and parcel of polycentric governance, as is explored further in Part IV, but it also highlights the difficulty of concerted action without a defined hierarchy in place, as seen in the Obama Administration and FTC's push for a federal data-breach-notification statute. Before discussing such matters in more detail, though, it is helpful to analyze the global context of this issue since: 1) many of these firms operate internationally, making them subject to varied regulatory approaches to IoT issues; and 2) other leading cyber powers, such as the European Union, have long studied the impact and importance of IoT, laying the groundwork for a potential cross-pollination of best practices. It is then to the role of comparative and international law that we turn to next before concluding with the more detailed study of polycentric governance in the IoT context.

last name, and one or more of the following data elements that are not encrypted or redacted: (A) a driver's license number; (B) a state identification card number; (C) a credit card number; and (D) a financial account number or debit card number in combination with a security code, password, or access code that would permit access to the person's account." IND. CODE § 24-4.9-2-10.

269. IND. CODE § 24-4.9-3-3.5(b) (emphasis added). Additionally, a data base owner is prohibited under the Indiana statute from "disposing of records or documents containing unencrypted and unreacted personal information of Indiana residents without shredding, incinerating, mutilating, erasing or otherwise rendering the personal information illegible or unusable." IND. CODE § 24-4.9-3-3.5(c) (2016).

270. OR. REV. STAT. § 646A.230, 646A.348; TEX. BUS. & COM. CODE ANN. § 521.151(a).

271. IND. CODE § 24-4.9-4-2.

272. FLA. STAT. § 501.171 (2016). For further discussion, see Karen L. Booth, *What Makes Florida's New Data Breach Law Unique*, LAW360 (July 1, 2014, 10:46 AM), http://www.law360.com/articles/553234/what-makes-florida-s-new-data-breach-law-unique.

D. Applicable Comparative and International Law to Enhancing the Security of Things

For the first time, the number of "things" connected to the Internet has surpassed the number of living people.[273] Yet, we are still only at the beginning of this technological transformation with tens of billions more IoT devices set to come online in the years ahead.[274] A recent European Commission study estimates that the market value of the IoT in the European Union alone is set to exceed one trillion euros by 2020.[275] As a result of the anticipated exponential growth in IoT, an array of EU organizations, regional associations, legal institutions, and commissions have begun to explore the risks and needs associated with a highly connected world. Yet, despite some progress, in many ways IoT remains largely unregulated in Europe.

This Section briefly explores the international regulation and policy approaches that have been adopted, or that are pending, by the EU, Japan, South Korea, and Australia as they relate to safeguarding security and privacy in the IoT context.[276] First, recent EU IoT initiatives are analyzed. Second, these findings are compared and contrasted with those from Japan, South Korea, and Australia, since these nations are among those considering IoT regulations within the national cybersecurity strategies and in domestic regulations. Finally, the Section considers associated issues within IoT such as big data and privacy considerations, including the convergence of soft-law regulation with hard-law mandates across these countries.

1. European Union IoT Policies

The EU cybersecurity regulatory structure is developing in a similar manner to the NIST framework developed in the United States. In fact, at the fifth Network and Information Security Directive ("NIS") Platform Plenary Meeting in Brussels, version two of the NIS Platform ("NISP") was introduced, which specifically adopts the NIST core—identify, protect, detect, respond, recover—as the industry-standard EU approach for enterprise risk management.[277] In December 2015, a tenta-

273. FTC IoT Report, *supra* note 195.

274. *Id.*

275. IDC Italia S.r.L & TXT e-solutions S.P.A., *Definition of a Research and Innovation Policy Leveraging Cloud Computing and IoT Combination*, EU COMM'N (May 13, 2015), https://ec.europa.eu/digital-agenda/en/news/definition-research-and-innovation-policy-leveraging-cloud-computing-and-iot-combination.

276. These particular national case studies were selected based on their size and importance, and to demonstrate the various regulatory styles being adopted. There is information that has been intentionally excluded from this analysis due to space constraints.

277. NIS PLATFORM, NETWORK AND INFORMATION SECURITY RISK MANAGEMENT ORGANISATIONAL STRUCTURES AND REQUIREMENTS 14 (2015), https://resilience.enisa.europa.eu/nis-platform/shared-documents/5th-plenary-meeting/chapter-1-nis-risk-management-organisational-structures-and-requirements-v2/at_download/file.

tive deal was reached on the NIS directive that would: 1) oblige EU Member States to develop national cybersecurity strategies and Computer Security Incident Response Teams; 2) engage in international information sharing; 3) require reasonable security measures and incident reporting for cyber attacks on critical infrastructure.[278] With this directive, the EU has moved to boost cybersecurity across Europe by agreeing to new rules obliging businesses to strengthen their defenses and forcing companies such as Google and Amazon to report attacks.[279] "'Critical operators' in industries including energy, transport, health and banking, 'will have to fulfill security measures and notify significant cyber incidents.'"[280] Simply put, the NIS directive comprises the "first ever EU-wide cybersecurity rules."[281] The process that led to the NIS directive is similar to deliberations involving the NIST framework, which included four public-private partnerships in which hundreds of businesses and policy-makers from the U.S. and around the world got together to build and revise the NIST framework, showing a remarkable ability to build consensus across numerous sectors and stakeholders in a complex and dynamic arena.[282] Many commentators argue that this "type of active dialogue is a crucial piece of the NIST framework's success—as well as that of the more general bottom-up approach to cybersecurity regulation—in the United States, and it is one that other nations are seeking to emulate."[283] Arguably, a similar effort is needed in the IoT context in particular.

278. *See* Günther H. Oettinger, *First EU-Wide Legislation on Cybersecurity Agreed*, EUR. COMM'N: BLOG (Dec. 8, 2015), https://ec.europa.eu/commission/2014-2019/oettinger/blog/first-eu-wide-legislation-cybersecurity-agreed_en.

279. *MEPs Close Deal with Council on First Ever EU Rules on Cybersecurity*, EUR. PARLIAMENT NEWS (Dec. 7, 2015), http://www.europarl.europa.eu/news/en/news-room/content/20151207IPR06449/html/MEPs-close-deal-with-Council-on-first-ever-EU-rules-on-cybersecurity.

280. Ian Wishart, *EU Strikes Cybersecurity Deal to Make Companies Boost Defenses*, BLOOMBERG: TECH (Dec. 8, 2015, 4:05 AM), http://www.bloomberg.com/news/articles/2015-12-08/eu-strikes-cybersecurity-deal-to-make-companies-boost-defenses.

281. *Id.*

282. *See Cybersecurity Framework Frequently Asked Questions*, NAT'L INST. OF STANDARDS & TECH. (May 29, 2016), http://www.nist.gov/cyberframework/cybersecurity-framework-faqs.cfm ("Among other things, the EO directed NIST to work with industry leaders to develop the Framework. The Framework was developed in a year-long, collaborative process in which NIST served as a convener for industry, academia, and government stakeholders. That took place via workshops, extensive outreach and consultation, and a public comment process. NIST's future Framework role is reinforced by the Cybersecurity Enhancement Act of 2014 (Public Law 113-274), which calls on NIST to facilitate and support the development of voluntary, industry-led cybersecurity standards and best practices for critical infrastructure. This collaboration continues as NIST works with stakeholders from across the country and around the world to raise awareness and encourage use of the Framework.").

283. Scott J. Shackelford et al., *Bottoms Up: A Comparison of "Voluntary" Cybersecurity Frameworks*, __ UNIV. CAL. DAVIS BUS. L.J. __ (forthcoming).

a. A Primer on the European Approach to Cybersecurity Regulation

The industry focused, bottoms-up approach to cybersecurity policymaking in the EU is not universal—some critics, for example, argue that EU regulatory efforts remain too centralized—still, progress is being made.[284] For example, in 2014 the European Commission funded a project entitled CIPHER, which conducted an "in-depth analysis of the reality of security in privately held information systems (PHIS) in Europe."[285] CIPHER served two main functions: 1) developing a methodological framework to help prevent cybercrime, and 2) drafting a global European regulatory and technological roadmap, containing recommendations for policy-makers.[286] For the purposes of the IoT, it is likely the second function is most germane to the current discussion.[287] Indeed, the Cyber Security Framework that forms part of CIPHER[288] offers a set of guidelines and recommendations to improve cybersecurity in systems that store or process the personal information of users.[289] The 2013 EU Cybersecurity Strategy introduced the NIS directive's goal to "facilitate exchange of best practices," enhance "risk management practices and information sharing"[290] through the establishment of the NIS Public-Private Platform ("NIS Platform").[291] This Platform helped collect "existing risk management standards and best practices"[292] which organizations "can use and tailor to their own approach to risk management."[293]

Aside from the NIS directive and pending General Data Privacy Directive, among the most important developments with regards to EU cybersecurity policymaking to date is the creation of the Digital Single

284. Press Release, Response to EU Cybersecurity Strategy and Proposed Directive on Network and Information Security (NIS) (Feb. 7, 2013), http://pr.euractiv.com/pr/response-eu-cybersecurity-strategy-and-proposed-directive-network-and-information-security-nis ("Member States are building communities and trust through local, regional, or sector specific private public partnerships, yet we see a general change in approach in the draft Network and Information Security Directive from working hand-in-hand with industry, to top-down, unidirectional reporting obligations and requirements.").

285. Eur. Comm'n Cmty. Res. & Dev. Info. Serv., *A Cyber Security Framework for Europe* (Aug. 5, 2014) [hereinafter *Framework*], http://cordis.europa.eu/news/rcn/121360_en.html.

286. *Id.*

287. *Id.*

288. CIPHER, *Integrated Cyber-Security Framework for Privately Held Information Systems and European Roadmap: D2.3–Methodological Framework* (2014), http://cipherproject.eu/wp-content/uploads/2014/05/CIPHER_D2.3_final1.pdf.

289. *Framework*, *supra* note 285 (The draft was evaluated by twenty experts from ten countries "working in various fields of cyber security and defence including experts in security engineering, experts in European regulations on data protection and experts in critical infrastructure protection"); *see generally* GEORGE CHRISTOU, CYBERSECURITY IN THE EUROPEAN UNION: RESILIENCE AND ADAPTABILITY IN GOVERNANCE POLICY (2015).

290. See Shackelford et al., *Bottom's Up*, *supra* note 283.

291. European Union Agency for Network & Info. Security, *Network and Information Security Risk Management Organisational Structures and Requirements* (Final Draft 220515), https://resilience.enisa.europa.eu/nis-platform/shared-documents/5th-plenary-meeting/chapter-1-nis-risk-management-organisational-structures-and-requirements-v2/view.

292. *Id.* at 5.

293. *Id.*

Market ("DSM"). The focus of the DSM is to tear down the regulatory walls and move from twenty-eight national markets to a single EU one.[294] Similar to the NIST framework, which "relies on a variety of existing standards, guidelines, and practices to enable critical infrastructure providers to achieve resilience,"[295] the DSM synthesizes initiatives on security and data protection.[296] Most importantly, the DSM focuses its approach upon considerations of the "data economy (free flow of data, allocation of liability, ownership, interoperability, usability and access), and thus promises to tackle interoperability and standardization" issues that are critical to boosting the Security of Things.[297]

b. European IoT Regulation

Specific to the IoT landscape, the European Commission has recently funded the Alliance for Internet of Things Innovation ("AIOTI"), which has been tasked with developing a large-scale framework specifically addressing issues within IoT.[298] The AIOTI Working Group delineated three possible approaches to policy creation, which, although captured within different terminology, seem to reflect conceptually the approaches considered in the creation of both the NIST framework and NIS directive. These approaches are included in Table 3.

294. Eur. Comm'n, Digital Single Market: Bringing Down Barriers to Unlock Online Opportunities [hereinafter DSM], http://ec.europa.eu/priorities/digital-single-market/index_en.htm (last visited Dec. 27, 2016).

295. Nat'l Inst. of Standards & Tech., Framework for Improving Critical Infrastructure Cybersecurity (Feb. 12, 2014), http://www.cslawreport.com/files/2015/04/07/nist-combined-file.pdf; *see Framework for Improving Critical Infrastructure*, NIST 4 (Apr. 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").

296. *See* DSM, *supra* note 294.

297. BUILDING THE HYPERCONNECTED SOCIETY: INTERNET OF THINGS RESEARCH AND INNOVATION VALUE CHAINS, ECOSYSTEMS AND MARKETS 2 (Ovidiu Vermesan et al. eds., 2015).

298. Alliance for Internet of Things Innovation, AIOTI Working Group 4–Policy (2015) [hereinafter AIOTI WG 4], https://www.vodafone.com/content/dam/group/policy/downloads/AIOTI-WG4-Policy-FINAL-151015-for-Publication.pdf.

TABLE 3. IOT POLICY OPTIONS PRESENTED TO THE EUROPEAN COMMISSION IN MAY 2013[299]

Option	EC activity	Efficiency	Efficacy
No action	Current trajectories continue	No guarantee for development in accordance with EU objectives	Market players retain complete freedom
Soft law	Using monitoring, innovation policy, industrial policy	If sufficient incentives for adoption and uptake exist, high effectiveness is possible, while incentivising coherence with EU policy objectives	Market players retain some freedom in deciding the most effective manner of complying with requirements
Hard law	Harmonisation and enforcement in IoT-related areas (e-commerce, data protection etc)	Depending on enforcement, mandatory compliance can be highly efficient	Negative externalities are hard to foresee given the early stage of technology development, therefore are difficult to avoid in legislation

Ultimately, the AIOTI Working Group determined that the middle course of "initial soft law approach combining standards, monitoring, 'information remedies' and an ethical charter to facilitate IoT self-organisation [sic] and clarify the need for and nature of effective regulatory interventions" was the most desirable.[300] Such a soft-law approach, which largely mirrors the U.S. Senate resolution discussed above,[301] allows for the development of an industry-focused framework, and, as such, is highly flexible, even as it could lead to the haphazard uptake of best practices as is discussed further in Part IV. Moreover, the soft-law-first regulatory approach leads to some potential overlap with existing EU privacy law.[302]

299. *Id.* at 6.
300. *Id.* at 6 (footnote omitted).
301. *See supra* Part III.B.
302. For example, the *Proposal for a Regulation of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data* (General Data Protection Regulation) (June 2015) is often considered the main source of regulatory guidance. The GDPR characterizes IoT as presumptively involving the cross-fertilization of data, individualized approaches, ubiquitous devices. In most instances these occurrences happen without user interfaces and involve the free flow of data. As such, the AIOTI recommends that "data protection legislation should consider the context of data use and reasonable expectations of users, and not take overly-prescriptive approaches to purpose limitation, notice, consent, profiling and cross border transfer." AIOTI WG 4, *supra* note 298, at 8. As of this writing, the GDPR is undergoing changes, the current draft uses privacy impact assessments and places emphasis on the use of codes of conduct intended to embody privacy by default and by design principles. *Id.* at 7 (citing *Article 29 Working Party - Opinion 8/2014 on the Recent Developments on the Internet of Things* (Sept. 2014)).

c. EU Big-Data Policy

Any discussion of European IoT policy also requires consideration of "Big Data." Across the EU, in national Big Data or IoT strategies, cybersecurity strategies and a number of other initiatives, have all addressed security in IoT or adjacent spaces,[303] such as European mandates on cybersecurity standardization.[304] After a review of existing frameworks, research-group work, and current regulation, the AIOTI Policy Working Group identified four policy objectives to guide policy creation regarding IoT and Big Data. First, the Working Group notes that IoT applications have different connectivity requirements, and these differences should be reflected in the level of security required.[305] For example, some IoT applications operate on a single platform or device, whereas others operate on multiple platforms and devices, demonstrating the need for policy that reflects "scales of security" based on various IoT application types.[306] Moreover, these differences in IoT applications should not be viewed in isolation; instead, focus should be placed on an application's ability to "offer an adequate, affordable and 'desired' security level relevant to each application, matching users' needs and business requirements."[307] A sliding-scale approach is therefore feasible in that some applications use less sensitive information, and, as such, these applications should be allowed to keep security-related costs to a minimum. Finally, while flexibility in the regulatory regime is necessary to ensure continued innovation,[308] at no time should essential security and privacy protections be compromised. Thus, all data-and privacy-based regulation should ensure that confidentiality, integrity, availability, and anonymity[309] remain the primary focus of regulatory efforts. For example, in relation to PII, the AIOTI Policy Working Group stated that privacy-impacting IoT applications[310] should guarantee "privacy and confidentiality of [the] data exchanged through or in transit on the networks or stored in the IoT application or in the Cloud."[311] Moreover, IoT applications must ensure data authenticity[312] and preserve the "integrity of a connected device (or system) for trustable solutions and services."[313]

303. AIOTI WG 4, *supra* note 298, at 16.
304. Such as those pursued in ETSI, CEN, and CENELEC.
305. AIOTI WG 4, *supra* note 298, at 18.
306. *Id.*
307. *Id.*
308. *Id.*
309. *Id.*
310. *Id.*
311. *Id.*
312. *Id.* (This is required "to enable trustable exchanges (from data emission to data reception. . .)").
313. *Id.*

d. The Internet of Everything EU Policy Convergence

On October 13, 2015, the European Commission launched specific actions to unleash the potential of the IoT within Focus Areas entitled Horizon 2020. Horizon 2020 will focus on the "following cross-cutting calls: (i) Industry 2020 in the Circular Economy, (ii) Internet of Things, and (iii) Smart and Sustainable Cities[,]" promoting improved congestion management, emergency response, and urban planning.[314] The goal of the latter initiative will be to "integrate smart homes, energy efficiency measures, very high shares of renewables, smart grids, energy storage, electric vehicles and smart charging infrastructures, using latest generation ICT platforms (and infrastructure) based on open specifications."[315] In short, the EU is embracing the "Internet of Everything," including wearables, which are "integrating key technologies (*e.g.*, nano-electronics, organic electronics, sensing, actuating, localization, communication, energy harvesting, low power computing, visualization and embedded software) into intelligent systems to bring new functionalities into clothes, fabrics, patches, watches, and other body-mounted devices."[316] These smart products assist people in monitoring their health, situational awareness, and decision-making, among other tasks. Horizon 2020 calls for particular attention to be paid toward providing, whenever feasible, fully automated closed-loop solutions, especially in the areas of healthcare, well-being, safety, security, and infotainment applications, to boost the Security of Everything.[317] Although, in its early stages, initiatives such as Horizon 2020 demonstrate a much wider use of IoT then previously envisioned, demonstrating that the IoT may well become the Internet of Everything.[318]

e. Other Notable IoT Regimes

Of the thirty-four national cybersecurity strategies published and available in English as of October 2015, only four (or 12% of the total) reference the Internet of Things: Japan, Austria, the Netherlands, and Italy. Only Japan, however, discusses the Internet of Things in any detail (Italy, for example, only references IoT in the appendix to its strategy,[319]

314. EUR. COMM'N, HORIZON 2020 WORK PROGRAMME (Oct. 13, 2015), http://ec.europa.eu/digital-agenda/sites/digital-agenda/files/discussions/h2020-wp1617-focus_en.pdf.

315. *See id.*

316. *Id.*

317. *Id.* at 93.

318. The Presidency of the Council of Ministers, and the Italian framework, as early as 2013 gave definition to the 'Internet of Things' and the 'Internet of Everything.' PRESIDENCY OF THE COUNCIL OF MINISTERS, NATIONAL STRATEGIC FRAMEWORK FOR CYBERSPACE SECURITY 42–43 (2013), https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/IT_NCSS.pdf. In contrast, Japan uses the term 'Machine to Machine' and does not draw a bright line distinction between the two concepts. GOV'T OF JAPAN, CYBERSECURITY STRATEGY 14 (2015) [hereinafter 2015 JAPAN CYBERSECURITY STRATEGY], http://www.nisc.go.jp/eng/pdf/cs-strategy-en.pdf .

319. PRESIDENCY OF THE COUNCIL OF MINISTERS, *supra* note 318, at 42.

while Austria simply notes the growth of the IoT).[320] Japan has engaged in the creation of a cybersecurity strategy that emphasizes bottom-up, voluntary private sector "self-governance."[321] While the Japanese approach to cybersecurity has involved relatively little direct regulation,[322] its cybersecurity strategy creates incentives for businesses within industry that demand strong cybersecurity to invest in the creation and development of robust cybersecurity practices.[323] Using, as an example, the development of IoT devices, the strategy[324] specifies that "the Government will promote security measures for these systems in a cross-sectoral manner, based on the Security by Design approach, and will give its prioritized support to the growth of such new business."[325] Moreover, Japan's strategy affirms a commitment to a bottom-up, collaborative approach to cybersecurity policy-making, and it emphasizes the importance of the various stakeholders coming together to develop standards by which they will hold themselves accountable.[326] In a manner similar to U.S. NIST framework and EU NIS directive, the strategy places a high emphasis on cross-sectoral involvement in the development of IoT cybersecurity standards.[327]

In contrast, and to demonstrate the regulatory spectrum emerging with regards to comparative cybersecurity policy-making, although not IoT specific, South Korea has historically taken a more hands-on approach to cybersecurity regulation than either the United States or Japan, combining strong broad-spectrum legislation protecting PII with sector-specific regulations governing other aspects of cybersecurity.[328] But, as highlighted in Table 3, the use of hard-law instruments is often criticized in situations where rapid development of expanded regulation

320. FED. CHANCELLERY OF THE REP. OF AUSTRIA, AUSTRIAN CYBER SECURITY STRATEGY 6 (2013), https://www.bka.gv.at/DocView.axd?CobId=50999.

321. 2015 JAPAN CYBERSECURITY STRATEGY, *supra* note 318, at 9.

322. While Japan does provide basic privacy protections, and requires that data controllers "take necessary and proper measures for the prevention of leakage, loss, or damage, and for other security control of the personal data," the implementation of these laws is left to sector-specific agencies, of which there are twenty-seven, whereas common protections, like data-breach notifications, are often absent or only recommended. This regulatory framework largely seeks to promote cybersecurity without imposing it. BAKERHOSTETLER, 2015 INTERNATIONAL COMPENDIUM OF DATA PRIVACY LAWS 109–10 (2015), http://towerwall.com/wp-content/uploads/2016/02/International-Compendium-of-Data-Privacy-Laws.pdf.

323. 2015 JAPAN CYBERSECURITY STRATEGY, *supra* note 318, at 13.

324. INFORMATION SECURITY POLICY COUNCIL, CYBERSECURITY STRATEGY: TOWARDS A WORLD-LEADING, RESILIENT AND VIGOROUS CYBERSPACE 10 (2013) (Japan) ("The rapid propagation of smartphones and other devices among people, 22, expansion of M2M/sensor networks, the advent of conditions where everything is connected to the internet (Internet of Things) and other situations, have increased the spread of the risks by introducing conditions where the devices which can be targeted by cyber attacks are present in every possible place and situation around us.").

325. 2015 JAPAN CYBERSECURITY STRATEGY, *supra* note 318, at 13.

326. *Id.*

327. *Id.* at 14.

328. *See, e.g.*, Personal Information Protection Act, Act No. 10465, Mar. 29, 2011, *amended* Aug. 6, 2013 (S. Kor.), *translated in* KoreanLII, http://koreanlii.or.kr/w/images/a/a3/PIPAct_1308en.pdf.

is a necessity, which is oftentimes the case regarding IoT issues.[329] Fortunately, the hard-law regulatory approach taken within the existing South Korean cyber-regulatory structure may be taking a more bottoms-up approaches with incentives for businesses to enhance their cybersecurity preparedness. The early success of these regulatory approaches has influenced the South Korean Ministry of Science to use a new means of authentication,[330] signaling a willingness to move South Korea cybersecurity policy into a more private-sector driven direction.

Elsewhere in Asia, though, other emerging markets have been taking quite different approaches to cybersecurity regulation. To take one example from Southeast Asia, Thailand, in contrast to Japan, has only embryonic cybersecurity regulations in place with an array of agencies ranging from the Royal Thai Police to the Department of Special Investigation and the Central Institute of Forensic Science, all contributing to the promotion of Thai cybersecurity.[331] The Thai government is also drafting various bills related to cybersecurity—perhaps owing to the nation's status as the eleventh-most-attacked nation in the world, according to one 2016 study[332]—including the Electronic Transactions Act and the Computer Related Crimes Act, which focus on providing security recommendations for organizations to conduct electronic transactions and combat cybercrime.[333] These Acts encourage both public and private organizations to have security and privacy policies, but they do not empower any agency to enforce organizations to do so.[334] As such, there is ample scope for cybersecurity regulatory intervention in Thailand. To help meet this threat, the Thai government has undertaken a series of reform measures as part of an overarching "Thailand Digital Economy Pol-

329. *See, e.g.*, Gen Kanai, *The Cost of Monoculture*, MOZILLA IN ASIA WEBLOG (Feb. 27, 2007), https://blog.mozilla.org/gen/2007/02/27/the-cost-of-monoculture; Chico Harlan, *South Korea Is Stuck with Internet Explorer for Online Shopping Because of Security Law*, WASH. POST (Nov. 5, 2013), https://www.washingtonpost.com/world/asia_pacific/due-to-security-law-south-korea-is-stuck-with-internet-explorer-for-online-shopping/2013/11/03/ffd2528a-3eff-11e3-b028-de922d7a3f47_story.html.

330. Simon Sharwood, *South Korea to Nuke Microsoft ActiveX*, REGISTER (Apr. 2, 2015), http://www.theregister.co.uk/2015/04/02/south_korea_to_deport_microsoft_activex.

331. *See* ROYAL THAI GOV'T, THE CABINET MEETING ON TUESDAY JANUARY 6, 2015, http://www.thaigov.go.th/index.php/en/cabinet-synopsis-/item/88954-88954.html (last visited Dec. 27, 2016).

332. *Thailand Is 5th Highest Risk in Asia for Cybersecurity Threats*, PAYPERS (Feb. 29, 2016, 10:23 AM), http://www.thepaypers.com/digital-identity-security-online-fraud/thailand-is-5th-highest-risk-in-asia-for-cybersecurity-threats/763186-26 ("In 2015, network security provider FireEye and Singaporean telco Singtel released a report noting that Thailand was the most affected by malware attacks in Southeast Asia. 40% of observed organizations in Thailand were hit by advanced cyber-attacks in the first half of 2015. Compare that to the regional rate of 29% and the global rate of 20%.").

333. Regarding cybercrime, the Thai government is in the process of amending several acts, including the Computer Related Crime Acts of 2007. The Thai government has applied the law to shut down or block thousands of websites and to prosecute a number of Internet users. Many global companies, including Facebook and Google, decided not to invest in Thailand since Section 15 indicates of the Act declares that content owners or administrators are responsible for any crime on the platform, such as posting inappropriate content.

334. L. PLUS, LAWS ON DIGITAL ECONOMY AND CYBER SECURITY (2015), http://www.lawplusltd.com/download/Updated%20webformat%20Editorial%20on%20Thailand%20DE%20bills.pdf.

icy," which includes ten separate bills related to information and communication technology, cybersecurity, computer crimes, personal data protection, and telecommunications.[335] These bills each require review by the Thai Council of State and the National Legislative Assembly, which is expected (as of this writing) by late 2016.[336] One of these bills, in particular the so-called "Cybersecurity Bill," is the most relevant for the current discussion. Among the provisions in this bill that have been met with some controversy is the degree of "governmental power to access private information"[337] in the name of enhancing "cybersecurity."[338] The bill calls for the establishment of a "National Cybersecurity Committee" to better meet the multifaceted cyber threat facing Thailand.[339] As of June 2016, the persons empowered to serve on the committee come from national defense circles. Criticism has focused, in particular, on allowing representatives from civil rights groups and industry to ensure a balanced perspective.[340] Additional reform options could include defining the scope of powers envisioned under the bill, "and the circumstances under which the Office of the NCSC can compel a private sector actor to perform a specific action."[341] Finally, there have been calls to revise Section 35(3), which empowers "designated officials . . . to gain access to any private owed or government owed data without having any kind of legal approval."[342]

The Thai government, like the EU, has also recognized the need for an articulated IoT and concomitant Big Data policy.[343] According to an interview with the deputy director of Electronic Transactions Development Agency, there have been increasing incidents of malicious software

335. Worapat Patram, *Industrial Concerns on Cybersecurity Bill in Thailand*, INTEL (Jan. 4, 2016), http://blogs.intel.com/policy/2016/01/04/industrial-concerns-cybersecurity-bill-thailand.

336. *Id.*

337. *Id.*

338. According to Section 3 of the National Cybersecurity Act, "'Cybersecurity' means measures and operations that are conceived in order to maintain national Cybersecurity, enabling it to protect, prevent or tackle circumstances of cyber threats which may affect or pose risks to the service or application of computer network, internet, telecommunications network, or the regular service of satellites in ways that affect national security, which includes military security, domestic peace and order, and economic stability." National Cybersecurity Bill, Jan. 6, 2015, § 3 (Thai.), *translated by* Thai Netizen Network, https://thainetizen.org/wp-content/uploads/2015/03/cybersecurity-bill-20150106-en.pdf.

339. *Id.* § 6; Patram, *supra* note 335 (This committee shall have the power to "order any of government and/or private entity to take any necessary and appropriate action to prevent and solve cyber-attacks." These steps could include: (1) a requirement to send a letter demanding clarification from a private or public entity regarding compliance with the Act; (2) to assist the committee in its actions to uphold the Act; (3) to access information, either in print or online, that would benefit national cybersecurity).

340. Patram, *supra* note 335.

341. *Id.*

342. *Id.*

343. Thailand has no regulation or policy related to Big Data. According to an interview, the government has been trying to push the Personal Data Protection Bill, which will regulate the process of the collection, utilization, and disclosure of personal data. The government encourages the industry to come up with "self-regulation" and follow privacy standards, such as Fair Information Practice Principles ("FIPPs"). Interview with Dr. Chaichana Mitrpant, deputy director, Thailand Electronic Transactions Development Agency, in Bangkok, Thailand (June 24, 2016).

targeting smart devices such as smartphones, smart homes, and smart cars.[344] The government encourages manufacturers to comply with international security standards such as NIST and ISO.[345] Many Thai manufacturers, however, have not followed these security standards, and the government does not have any authority to force the companies to comply.[346] When asked about the approach to IoT regulation, the officials mentioned that the industries should come up with "self-regulation" rather than regulations by the government, highlighting an approach similar to Japan and other Asian neighbors.[347]

By way of a final comparative regulatory approach, the Australian model of cybersecurity regulation could be described as a mix between that of the EU and the U.S., employing a small number of broad-spectrum data-protection laws, which are supplemented with sector-specific laws in areas of heightened cybersecurity concern.[348] Australia developed a cybersecurity strategy in 2009[349] with the creation of a National Security Strategy in 2013.[350] At the time of release, Australia's Prime Minister Julia Gillard proclaimed the "[g]overnment will focus on delivering integrated cyber policy and operations to deal with these developments in the context of its broader digital agenda."[351] And since that time, it seems Australia has been hard at work to engage local and regional efforts to enhance cybersecurity. For example, Australia has recently undertaken a comprehensive cybersecurity review, scheduled to release by the end of 2015, designed to better address cybersecurity concerns in this evolving cyber-landscape. Australian government agencies already recommend the NIST framework,[352] thus, commentators are asserting that the recommendations will incorporate elements of this initiative.[353] For example, early discussions have focused on the creation of a national voluntary cybersecurity standard, which will define the various levels of cybersecurity preparedness, including within the IoT context.[354] The use of such a broadly bottom-up regulatory approach demonstrates a commitment to self-regulation and allows firms (at least outside of the

344. *Id.*
345. *Id.*
346. *Id.*
347. *Id.*
348. Alexandra T. McKay, *The Private Sector Amendment to Australia's Privacy Act: A First Step on the Road to Privacy*, 14 PAC. RIM. L. & POL'Y J. 223, 224 (2005).
349. AUSTL. GOV'T, CYBER SECURITY STRATEGY (2009), http://www.ag.gov.au/RightsAndProtections/CyberSecurity/Documents/AG%20Cyber%20Security%20Strategy%20-%20for%20website.pdf.
350. Zeljka Zorz, *Australia's First National Security Strategy Emphasizes Cyber Defense*, HELP NET SECURITY (Jan. 23, 2013), http://www.net-security.org/secworld.php?id=14288.
351. *Id.*
352. AUSTL. SEC. & INVESTMENTS COMM'N, CYBER RESILIENCE: HEALTH CHECK (Mar. 2015), http://download.asic.gov.au/media/3062900/rep429-published-19-march-2015-1.pdf.
353. *See* Robert Parker, *Developing and Australian Cybersecurity Framework*, AUSTRALIAN: BUS. SPECTATOR (Sept. 18, 2015, 9:38 PM), http://www.businessspectator.com.au/article/2015/9/18/technology/developing-australian-cybersecurity-framework.
354. *Id.*

critical infrastructure context) to determine an appropriate level of cybersecurity for their business needs and risk-tolerance profiles.

E. Summary

This Part has examined applicable federal, state, and comparative international law related to IoT governance. In all, although progress is being made, such as in defining what constitutes "reasonable" cybersecurity practices under FTC Act Section 5(a), governance gaps remain in numerous sectors—including retail and healthcare—requiring more effective self-regulation until black-letter law catches up with ongoing technological changes. The final Part analyzes the prospect of polycentric regulation to enhance the Security of Things before concluding with a discussion of implications for both managers and policy-makers.

IV. LEVERAGING POLYCENTRIC APPROACH TO ENHANCE THE SECURITY OF THINGS

As Parts II and III helped illustrate, despite the continuing evolution of law and policy in the IoT context, including some areas of convergence, IoT governance remains underdeveloped. In fact, the Information Systems Audit and Control Association ("ISACA")[355] surveyed IT professionals in the United Kingdom 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 standards in the industry do not sufficiently address IoT *specific* security concerns."[356] IoT may begin to enjoy heightened regulatory attention, but for the time being, as seen in both the U.S. Senate resolution as well as in the EU and Japan, there is a growing consensus that bottoms up cybersecurity frameworks featuring a high degree of private-sector control and coordination are the best soft approach to enhance the Security of Things for the foreseeable future. In an effort to help boost the odds of success for such frameworks, this Part examines the literature on polycentric governance focusing on the IAD-SES Framework and new governance notions before concluding with an examination of implications.

A. An Introduction to Polycentric Governance and the IAD-SES Framework

Beginning in the early 1990s with her groundbreaking book *Governing the Commons*, Professor Elinor Ostrom created an informative

355. Previously known as 'Information Systems Audit and Control Association,' http://www.isaca.org/about-isaca/Pages/default.aspx (last visited Dec. 27, 2016).

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

framework of eight design principles for the management of common-pool resources known as the Institutional Analysis and Design ("IAD") Framework.[357] These principles include the importance of: 1) "clearly defined boundaries for the user pool . . . and the resource domain";[358] 2) "proportional equivalence between benefits and costs;"[359] 3) "[c]ollective choice arrangements" ensuring "that the resource users participate in setting . . . rules";[360] 4) "[m]onitoring . . . by the appropriators or by their agents";[361] 5) "[g]raduated sanctions" for rule violators;[362] 6) "[c]onflict-resolution mechanisms [that] are readily available, low cost, and legitimate";[363] 7) "minimal recognition of rights to organize";[364] and 8) "governance activities [being] . . . organized in multiple layers of nested enterprises."[365] Not all of Professor Ostrom's design principles are applicable in the IoT context since they were designed primarily for managing small-scale common-pool resources, such as forests and lakes. Some do have salience, however, and are addressed in turn to inform a discussion of appropriate policy responses to boosting the Security of Things.

1. Defined Boundaries

According to Professor Ostrom, "[t]he boundary rules relate to who can enter, harvest, manage, and potentially exclude others' impacts. Participants then have more assurance about trustworthiness and cooperation of the others involved."[366] In the IoT context, defined boundaries are especially problematic given the extent to which various smart devices from automobiles to thermostats and even toasters interconnect, together forming an ecosystem that has its ultimate manifestation in the Internet of Everything discussed in Part III.[367] As such, trust can only be built in such a landscape by segmenting the IoT into smaller micro communities,[368] such as through smaller forums, perhaps building from sector-

357. *See* ELINOR OSTROM, GOVERNING THE COMMONS: THE EVOLUTION OF INSTITUTIONS FOR COLLECTIVE ACTION 90 (James E. Alt & Douglass C. North eds., 1990).

358. SUSAN J. BUCK, THE GLOBAL COMMONS: AN INTRODUCTION 32 (1998) (emphasis removed).

359. *See* OSTROM, *supra* note 357, at 90.

360. BUCK, *supra* note 358, at 32 (emphasis removed).

361. *Id.* (emphasis removed).

362. *Id.* (emphasis removed).

363. *Id.* (emphasis removed).

364. 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.53 (Eric Brousseau et al. eds., 2012) (emphasis removed).

365. *Id.*

366. *Id.* at 119.

367. *See supra* Part III.C.

368. *See supra* Part III.A.

specific Information Sharing and Analysis Centers ("ISACs") or broader ISAOs.[369]

2. *Proportionality*

This design principle underscores the need for equity in a system so that some of the "users [do not] get all the benefits and pay few of the costs. . . ."[370] This is a frequent refrain in the cybersecurity context with few providers wishing to invest as much as perhaps they should in proactive cybersecurity measures because the full benefits of such investments are not internalized to the firm. Under this argument, cybersecurity is a public good, and if cyber attacks do not result in increased cybersecurity investments, then there exists an IoT market failure necessitating some form of governmental intervention to correct.[371]

3. *Collective-Choice Arrangements and Minimal Recognition of Rights*

Professor Ostrom's third design principle 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."[372] This principle implies the importance of engaged and proactive rulemaking by technical communities, the private sector, and the international community.[373] This criterion, at least, has been on display in the IoT context as seen in the 2014 NIST Framework, the 2015 NIST IoT Framework, and the 2015 EU NIS Directive, all of which included active private-sector engagement throughout the policy formulation process.

4. *Monitoring*

According to Professor Ostrom, trust can typically only do so much to mitigate rule-breaking behavior.[374] Eventually, some level of monitor-

369. *Information Sharing and Analysis Organizations (ISAOs)*, DEP'T HOMELAND SEC., http://www.dhs.gov/isao (last visited Dec. 27, 2016).

370. Ostrom, *supra* note 364, at 120.

371. *See* Robert Beeres & Myriame Bollen, *An Economic Analysis of Cyber Attacks*, *in* CYBER WARFARE: CRITICAL PERSPECTIVES 147, 153 (Paul Ducheine et al. eds., 2012) (discussing cyber security as a public good and, thus, we could define it as "the goods, services, measures, techniques that aim to enhance the feeling of being secure in cyberspace"); Eli Dourado & Jerry Brito, *Is There a Cybersecurity Market Failure?*, 106 MERCATUS ON POL'Y 2 (2012), https://www.mercatus.org/sites/default/files/Cybersecurity_DouradoBrito_MOP_Final.pdf (arguing that market failures are not so common in the cybersecurity realm); Jennifer Booton, *3 Reasons Why Cyberattacks Don't Hurt Stock Prices*, MARKET WATCH (Apr. 3, 2015, 1:33 PM), http://www.marketwatch.com/story/3-reasons-why-cyberattacks-dont-hurt-stock-prices-2015-04-03.

372. Ostrom, *supra* note 364, at 120.

373. *See* George J. Siedel & Helena Haapio, *Law as a Source of Strategic Advantage: 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").

374. Ostrom, *supra* note 364, at 120.

ing becomes important. In self-organized communities, typically monitors are chosen among the members to ensure "the conformance of others to local rules."[375] To help reinforce this principle in the IoT context, norm entrepreneurs could volunteer to help establish best practices and mechanisms for rule-breakers. This role could also be fulfilled by the courts as litigation emerges in the aftermath of the Wyndham ruling and other state and federal actions (including those in response to new or revised state data-breach notification statutes) forming the contours of what constitutes a "reasonable" level of cybersecurity care for IoT operators.

5. Graduated Sanctions and Dispute Resolution

Other insights from Professor Ostrom's principles, such as the need for graduated sanctions for rule violators and effective dispute resolution, speak to the importance of addressing legal ambiguities and establishing norms of behavior.[376] The former point underscores the significance of not "[l]etting an infraction pass unnoticed,"[377] which again highlights the need for industry councils and close private-sector collaboration to police self-regulation with civil society potentially using public shaming to further incentivize the use of cybersecurity best practices.

6. IAD Summary

As helpful as the IAD Framework is at analyzing the factors necessary to create a functioning system of polycentric governance to help address a given global collective-action problem, it is far from perfect, as Professor Ostrom would be the first to admit.[378] Here, while collective-choice arrangements point to the potential to build trust in IoT sectors, the lack of defined boundaries, proportionality, and graduated sanctions calls into question the feasibility of effective self-regulation by itself to enhance the Security of Things. The IAD Framework, however, forms only one component of the literature on polycentric governance, and while Professor Ostrom's important work on the IAD Framework often gets much of the attention in public policy circles, given its emphasis on self-understanding beyond classical rational choice,[379] her work on the Social-Ecological-System ("SES") Framework, beginning in approximately 2007, offers an even more "comprehensive approach to the study

375. *Id.* at 121.
376. *Id.*
377. *Id.*
378. *See* Elinor Ostrom et al., *Revisiting the Commons: Local Lessons, Global Challenges*, 284 SCI. 278, 282 (1999) (noting that some of her work in the global commons context to "provide starting points for addressing future challenges").
379. Michael D. McGinnis, *Elinor Ostrom: Politics as Problem-Solving in Polycentric Settings*, *in* ELINOR OSTROM AND THE BLOOMINGTON SCHOOL OF POLITICAL ECONOMY 281, 292 (Daniel H. Cole & Michael D. McGinnis eds., 2014).

of closely-coupled systems" drawing from both social and ecological factors.[380]

7. Enter the IAD-SES Framework

In Professor Ostrom's own words, the SES Framework helps show "the relationships among four first-level core subsystems" including "resource systems . . . resource units. . governance systems . . . and users. . . ."[381] There are issues, however, with the SES Framework as well, including the fact that it is "[p]urely descriptive, diagnostic, and static," as well as the "absence of economic variables" and a "[d]ubious specifications of some variables."[382] Although work on a combined IAD-SES Framework continues as of this writing, early results, including those by Professors Dan Cole and Michael McGinnis, show great promise.[383] A combined IAD-SES Framework promises to be more dynamic, logically structured, and includes other factors such as transaction costs into the model's overarching design.[384] Potentially combining the IAD-SES Framework with other relevant literatures, such as "new governance," which seeks to move international law beyond traditional multilateral treaties to recognize the importance of unilateral, bilateral, and regional measures and the new work on changing beliefs opening up windows for institutional realignment, such as argued for by Professor Lee Alston,[385] that could further build out the conceptual core of IoT governance.[386]

B. Implications for Managers and Policy-makers

What does all of this mean for managers and policymakers? Simply put, a successful polycentric framework requires six general steps, as well as a number of IoT specific initiatives. First, there must be cooperation amongst stakeholders, including the sharing of information within defined boundaries and limitations on propriety system and software creation, along with graduated sanctions being in place for rule breakers. Second, active stakeholder participation, such as through collective-choice arrangements in the NIST framework and NIS directive processes, is vital to success. Third, proactive cooperation amongst stakeholders

380. *Id.*

381. Elinor Ostrom, *A General Framework for Analyzing Sustainability of Social-Ecological Systems*, 325 SCI. 419, 420 (2009).

382. DAN COLE ET AL., TOWARD A COMBINED IAD-SES FRAMEWORK 8 (2013).

383. *Id.*

384. *Id.* at 9.

385. *See, e.g.*, LEE J. ALSTON ET AL., BRAZIL IN TRANSITION: BELIEFS, LEADERSHIP, AND INSTITUTIONAL CHANGE 2–23 (2016).

386. *See, e.g.*, Kenneth W. Abbott & Duncan Snidal, *Strengthening International Regulation Through Transnational New Governance: Overcoming the Orchestration Deficit*, 42 VAND. J. TRANSNAT'L L. 501, 501 (2009) (defining "new governance" as a new kind of international regulatory system arising from the failure of "[o]ld [g]overnance" (*e.g.*, multilateral treaties and international organizations)).

and government agencies to react quickly to cybersecurity issues in the IoT context is also imperative, such as through broader, IoT-specific ISAOs as envisioned in the Cybersecurity Act of 2015.[387] Fourth, the use of flexible, guidance-driven frameworks without overly prescriptive regulatory language or technology-specific terminology is also desirable, as seen in both the U.S. Senate Resolution and EU Directives. Fifth, IoT providers must be willing to comply with industry standards without the need for governmental intervention to encourage good behavior, which can be accomplished by effective monitoring of peers and an active role for civil society in shaming outliers. Sixth, and finally, government should be willing to allow industry to react to data breaches without overly broad, harsh, or punitive fines, except in egregious circumstances, as has begun to be defined in the U.S. context through FTC Act Section 5(a) litigation.

Building from these steps, an overarching approach to enhancing the SoT is by conceptualizing IoT as an ecosystem and encouraging IoT providers to take responsibility for how their products impact the entire ecosystem, similar to how stakeholders operate in the SES context. Entities that are information gatherers, information aggregators, and information transmitters/communicators, for example, could be liable for misusing user data, especially when such misuse has downstream consequences or involves critical or highly sensitive information, much like employers are responsible for many employee actions.[388] The use of such an approach creates incentives for self-monitoring of the ecosystem and may encourage various industries across the IoT landscape to work together and gain a broader perspective on how IoT devices and data interact. The IoT ecosystem approach could help incentivize participants to develop and maintain appropriate levels of cybersecurity, and is flexible to information type and malleable to changes in the environment, even as it insists upon ecosystem monitoring and taking accountability for the entirety of the system. Industry outliers could also find it difficult to purchase and/or share information with cooperative industry participants, a real-life application of defined boundaries and user groups from the IAD Framework.

Moreover, lessons from related areas should not be ignored since device management issues that arise in IoT also come about within other analogous fields. Consider two recent examples: Google and Mattel. Turning to Google first, under the Family Educational Rights and Privacy Act a schools needs to obtain written consent from parents before sharing personal information about students, except when the school sharing data with "school officials" has a "legitimate educational inter-

387. Cybersecurity Information Sharing Act of 2015, S. 754, 114th Cong. (2015).

388. *See, e.g.*, OCCUPATIONAL SAFETY & HEALTH ADMIN., https://www.osha.gov/workers/index.html (last visited Dec. 27, 2016).

est" in the data.[389] This definition has been interpreted to include contractors, since schools now outsource some of their functions.[390] And, Google—it seems—falls under that definition.[391] The result is that Google has been gathering a great deal of information about students as a result of their use of certain Google products such as Droid-powered tablets, and it has been using that information within its own ecosystem of GoogleWorld, with parents having no ability to prevent such information gathering.[392] How Google will use, protect, and store this student information, how or with what data sources this information will be aggregated, and to whom it will pass on this information remain open questions as of this writing.

Mattel is another large corporate entity that has the ability to aggregate information across product lines and information sources. Yet, it seems unaware of the public's growing awareness of the 'creepy' factor in the emerging IoT landscape. In 2015, Mattel released "Hello Barbie," a smart doll with a microphone and Wi-Fi connectivity that allows Mattel to host two-way conversations with children.[393] And while one can assume the backlash was instant, in fact several privacy groups alerted individuals to the two-way communication feature in early 2015,[394] the doll was released without major modification in time for Christmas 2015.[395] This example serves as a reminder that industry self-monitoring can only serve as a mechanism to flag industry outliers; it cannot by itself change the behavior of multinational businesses that seek to take advantage of poorly constructed or antiquated policy, or individual user apathy.

Consequently, while it is true that the desire for industry self-regulation seems justified, given the still nascent state and rapid development of the underlying technologies, some IoT regulation may in fact be necessary, especially in critical areas of concern, such as transportation and healthcare. Regulation, however, should be limited to at-risk areas or populations (such as children), and it should be crafted to reinforce existing best-practice frameworks, as has arguably happened in the electricity regulatory context.[396] Most important to a self-regulatory model, policy-makers must create incentives to encourage the further refine-

389. Family Educational Rights and Privacy Act (FERPA), 20 U.S.C. § 1232g (2012); 34 C.F.R. § 99 (2015).

390. 34 C.F.R. § 99.5(c)(1).

391. *See* Andrea Peterson, *Google, a 'school official?' This Regulatory Quirk Can Leave Parents in the Dark*, WASH. POST (Dec. 30, 2015), https://www.washingtonpost.com/news/the-switch/wp/2015/12/30/google-a-school-official-this-regulatory-quirk-can-leave-parents-in-the-dark.

392. *Id.*

393. *See* Benjamin Snyder, *Activists Fight Release of New High-tech Barbie Doll from Mattel*, FORTUNE (Mar. 25, 2015 1:54 PM), http://fortune.com/2015/03/25/barbie-privacy-susan-linn.

394. *See* Alejandro Alba, *Mattel's Talking Hello Barbie Doll Raises Concern over Children's Privacy*, DAILY NEWS (Mar. 16, 2015 1:17 PM), http://www.nydailynews.com/news/national/mattel-barbie-raises-concern-children-privacy-article-1.2151019.

395. *See id.*

396. *See* INTELLIGENCE & NAT'L SEC. ALLIANCE, ADDRESSING CYBER SECURITY THROUGH PUBLIC-PRIVATE PARTNERSHIP: AN ANALYSIS OF EXISTING MODELS 7 (Nov. 2009), www.insaonline.org/i/d/a/Resources/Addressing_Cyber_Security.aspx.

ment of best practices as part of an ecosystem of information-system participants.

In the creation of the IoT regulatory interventions, policy-makers must recognize one important behavioral element; individuals often behave in a less-than-protective manner when it comes to what they share online. Consider the Wyndham as an example. Individuals continued to provide information to Wyndham after the breach was discovered but before litigation ensued. What should Wyndham (and others) take away from that fact? Unfortunately, one lesson is that people, in general, are oftentimes unwilling or incapable of protecting their own information, especially given the recent deluge of data breaches.[397] Yet, consumers are at risk in data breaches, especially in the IoT environment, and that fact serves as an insulator to information security accountability. Thus, the ability to blame user error or to limit accountability for due diligence based on general use-of-service consent needs to be questioned. People are predictably apathetic when it comes to their online behavior, such as reading terms and conditions.[398] As a result, businesses should accept some responsibility in protecting PII. For example, as previously discussed, the Health Insurance Portability and Accountability Act only covers patient information kept by health providers, insurers, and data clearinghouses, as well as their business partners, but these definitions are vague. The result, in January of 2015 Jacqueline Stokes discovered the home paternity test results of 6,000 unsuspecting people openly available online.[399] The individuals had consented to the use of the test and had agreed to receive their results online, but had not consented (without ever reading the terms of use) to the information being used in aggregate for research and other search activities. As this example illustrates, policy-makers need to create an information ecosystem that insists upon accountability while encouraging the reporting of data loss within a flexible regulatory model, and managers should be encouraged to plan for the likely behavior of users, for instance, by designing automatic security and privacy opt-out protections.

Further, more can be done to help set the stage for successful self-regulation consistent with the foregoing discussion of the IAD-SES Framework and related concepts such as new governance. First, the IoT needs to be unbounded so as to create natural boundaries for self-

397. *See World's Biggest Data Breaches*, INFORMATION IS BEAUTIFUL, http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks (last visited Dec. 27, 2016).

398. *See* Rebecca Smithers, *Terms and Conditions: Not Reading the Small Print Can Mean Big Problems*, GUARDIAN (May 11, 2011, 2:00 PM), http://www.theguardian.com/money/2011/may/11/terms-conditions-small-print-big-problems.

399. *See* Charles Ornstein, *Federal Privacy Law Lags Far Behind Personal-Health Technologies*, WASH. POST (Nov. 17, 2015), https://www.washingtonpost.com/news/to-your-health/wp/2015/11/17/federal-privacy-law-lags-far-behind-personal-health-technologies/?utm_term=.1ab7ce41fd12. Unfortunately, the tail of the lost medical information is a tale often told. For example, in 2011 an Australian company did not properly secure details of hundreds of paternity and drug tests, making them accessible through a public Google search. *Id.*

regulation within the areas of information types or sector-specific groupings. This would permit boundaries to be more fluid and regulation to be limited to those areas demanding the highest amount of security, determined by either information type or critical information categorization. Proportionality is ensured as those that handle the most sensitive information bear the burden of creating the most robust security, while ensuring that others within the ecosystem have equally robust systems and ensure sensitive information is not shared beyond the ecosystem. Moreover, while proportionality tells us that those who draw the greatest benefit from particular types of information should bear the burden of the cost associated with protecting it, the cost also creates incentives for those stakeholders to remain engaged in the decision-making process. External and community-based incentives to encourage reporting of IoT issues, along with external incentives to promote best practices should also be fostered. For example, while many ponder how Volkswagen was allegedly able to equip hundreds of thousands of its vehicles with special electronic equipment designed to evade emissions testing,[400] some may wonder why the industry itself did not self-police more effectively. It might be that the industry, with little incentive to report such a discrepancy, sought to achieve the same standard without necessarily questioning the accuracy of the Volkswagon data in the first place. Incentive systems encourage monitoring and allow for benefits to be recognized by those that are compliant and those that report the noncompliant. Incentives such as liability limitation for certain types of information sharing,[401] technical assistance, public-bug bounty programs, and offering priority consideration to certain federal grants all serve as examples of such incentives.[402]

Finally, policy-makers must consider instances where the industry simply cannot make the decisions about what to do with a given type of information within the IoT ecosystem. For example, consider the case of a Florida woman's car that informed authorities after she allegedly rear-ended two vehicles and left the scene without reporting the accident to the authorities.[403] In this instance, Ms. Bernstein had activated Ford's Emergency Assistance safety feature after she was involved in a "sudden

400. *See, e.g.*, *VW Emissions Scandal Latest: Renault Sites Investigated*, TOP GEAR (Jan. 14, 2016), http://www.topgear.com/car-news/insider/vw-emissions-scandal-latest-renault-sites-investigated.

401. This is already happening to an extent with the U.S. government encouraging automobile manufacturers to work with one another through a new Information Sharing and Analysis Center and with consumers and the government to identify and share cybersecurity best practices. *See* Pete Bigelow, *18 Automakers Agree on New Safety Pact with Regulators*, AUTO BLOG (Jan. 15, 2015), http://www.autoblog.com/2016/01/15/18-automakers-agree-new-safety-pact.

402. *See* Michael Daniel, *Incentives to Support Adoption of the Cybersecurity Framework*, WHITE HOUSE (Aug. 6, 2013), https://www.whitehouse.gov/blog/2013/08/06/incentives-support-adoption-cybersecurity-framework.

403. *See* Trevor Mogg, *Hit-And-Run Suspect Arrested After Her Own Car Calls Cops*, DIGITAL TRENDS (Dec. 7, 2015), http://www.digitaltrends.com/cars/hit-and-run-suspect-arrested-after-her-own-car-calls-cops.

change of speed or movement."[404] In these instances, the Emergency Assistance feature automatically places an emergency call to local first responders allowing emergency personnel to assist injured or otherwise incapacitated individuals. Unfortunately, Ms. Bernstein was neither, but was instead allegedly intent on leaving the scene of the accident.[405] While this information may be detrimental to Ms. Bernstein—and those similarly situated to her—such information must not be shielded from sharing given that it is serves a necessary public good—in this case, the promotion of traffic safety and accountability.

Regarding more specific takeaways for managers, it is vital to build in proactive cybersecurity best practices from the inception of a new IoT product line. The lesson here is constant vigilance, *e.g.*, letting an initial process of cybersecurity due diligence be the first, and not the last, word in an ongoing, comprehensive cybersecurity policy that promotes cyber hygiene along with the best practices essential for battling the multifaceted cyber threat.[406] Such a policy should be widely disseminated and regularly vetted as part of an overarching enterprise risk management process, along with having an incident response plan in place that includes private and public information sharing mechanisms.[407] These recommendations are in line with FTC guidance, as seen in the Wyndham settlement order,[408] which should be considered the ground floor of compliance to be supplemented by the 2014 NIST Framework and NIST IoT Framework to check for governance gaps that may then be filled in by industry best practices. Concrete steps for retailers, for example, in addition to the above, could include installing software to deactivate RFID tags after a pre-determined period of time so as to avoid consumer privacy concerns. Powershelves could similarly limit real-time location tracking to only specific applications. Health data should be encrypted from end-to-end to help get ahead of the HIPAA-HITECH Act regulatory curve. Voluntary, private-sector driven certification schemes could also be created to signal customers to those IoT companies that have taken such basic cybersecurity measures.[409]

Globally, in building from the new governance literature, minilateral partnerships should be fostered to help engender and spread trust among the increasing numbers of IoT participants. This is already hap-

404. *Id.*

405. *Id.*

406. *See* GREGORY J. TOUHILL & JOSEPH TOUHILL, CYBERSECURITY FOR EXECUTIVES: A PRACTICAL GUIDE 291 (2014) ("You should measure your cybersecurity posture as part of your efforts to practice due care and due diligence, monitor and control your information systems, maintain legal and regulatory compliance, meet contractual obligations, and maintain certifications.").

407. For more on this topic, see Amanda N. Craig et al., *Proactive Cybersecurity: A Comparative Industry and Regulatory Analysis*, 52 AM. BUS. L.J. 721, 722 (2015).

408. *See* Wyndham Settles, *supra* note 220.

409. *See* David Inserra & Steven P. Bucci, *Cyber Supply Chain Security: A Crucial Step Toward U.S. Security, Prosperity, and Freedom in Cyberspace*, HERITAGE FOUND. (Mar. 6, 2014), http://www.heritage.org/research/reports/2014/03/cyber-supply-chain-security-a-crucial-step-toward-us-security-prosperity-and-freedom-in-cyberspace.

pening to an extent, for several cross-border partnerships have emerged that may present yet another option to protect sensitive PII. For example, in December 2010, the U.S. Department of Health and Human Services ("HHS") and the European Commission's DG CONNECT signed a Memorandum of Understanding ("MoU") on Cooperation surrounding eHealth/Health IT.[410] The MoU was signed to demonstrate a shared dedication to strengthening transatlantic cooperation in eHealth and Health Information Technologies. In 2013, DG CONNECT and HHS published a first Roadmap of specific MoU actions.[411] Since then, this Roadmap has guided activities in two priority areas (work streams):

1. Standards development to advance the development and use of internationally recognized standards supporting transnational interoperability of electronic health information and communication technology; and
2. Workforce development to develop and expand the skilled Health IT workforce in Europe and the US.[412]

In 2015, DG CONNECT and the U.S. HHS agreed to add a third priority area: Transatlantic eHealth/Health IT Innovation Ecosystems.[413] This work stream aims to encourage innovation in the eHealth/Health IT industry and ensure linkages to the other two Roadmap work streams.[414] Over time, further linkages could be added to this and other IoT partnerships; indeed, the active collaboration surrounding the NIST framework could be extended with a special emphasis on IoT concerns as part of the growing bottom-up approach to enhance the Security of Things.

V. CONCLUSION

This Article has unpacked the technological evolution of the Internet of Things with a particular emphasis on the retail and healthcare sectors. It has also surveyed applicable state, federal, and international law to identify regulatory trends and to spot governance gaps. As we have seen, self-regulation is helping to assuage some ongoing cybersecurity and privacy concerns, but much more remains to be done to leverage the power of polycentric governance, including, with regards to the IAD-SES Framework and new governance literature, to conceptualize an effective bottom-up system for enhancing the Security of Things. Still, important steps are being taken, such as the 2014 NIST Framework, the

410. EUROPA, MEMORANDUM OF UNDERSTANDING (2010), http://ec.europa.eu/digital-agenda/en/news/memorandum-understanding-eu-us-ehealth.

411. EUROPA, TRANSATLANTIC EHEALTH/HEALTH IT COOPERATION ROADMAP (2013), http://ec.europa.eu/digital-agenda/en/news/transatlantic-ehealthhealth-it-cooperation-roadmap.

412. *Id.*

413. *Public Stakeholder Consultation on Next Phase of EU-US Cooperation in eHealth/Health IT* (Dec. 22, 2015), https://ec.europa.eu/digital-agenda/en/news/public-stakeholder-consultation-next-phase-eu-us-cooperation-ehealthhealth-it.

414. *Id.*

2015 NIST IoT Framework, FTC rulings regarding Section 5(a), the NIS directive, and the Japanese Cybersecurity Strategy. Together, these laws and policies can help drive the further evolution of effective and secure IoT governance, but the central role played by the private sector as both the lead technology developer and governance center should not be underestimated. It is thus critical to leverage the power of the private sector and civil society to foster cyber peace in the IoT before insecurity abounds in the Internet of Everything.[415]

415. *See* Shackelford et al., *Promote Cyber Peace*, *supra* note 27.