HAVE YOU UPDATED YOUR TOASTER?
TRANSATLANTIC APPROACHES TO GOVERNING THE INTERNET OF EVERYTHING

Scott J. Shackelford, JD, PhD*
Scott O. Bradner**

Abstract

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. The rise of "smart products" such as Internet-enabled refrigerators and self-driving cars holds the promise to revolutionize business and society. To substantiate the coming wave, Samsung has announced that *all* of its products would be connected to the Internet by 2020. Yet it is an open question whether security can or will scale along with this increasingly crowded field, or whether a combination of perverse incentives, increasing complexity, new problems, and new impacts of old problems like "technical debt" amassing from products being rushed to market, will derail progress and exacerbate cyber insecurity. This Article investigates contemporary approaches to IoT security through an in-depth comparative case study focusing on the European Union and the United States. Particular attention is paid to the impact of the General Data Protection Regulation (GDPR) and the Network Information Security (NIS) Directive in the EU, and influence of the National Institute for Standards and Technology (NIST) Cybersecurity Framework, and other leading standards, on IoT security with a focus on mitigating the risk of politically motivated attacks. We analyze transatlantic reform proposals—including the U.S. Internet of Things (IoT) Cybersecurity Improvement Act of 2017 and the potential for a dedicated NIST Framework for IoT security given the international success of the NIST CSF—and argue for a polycentric approach to boosting IoT securing across both jurisdictions by applying lessons from major Internet governance debates.

Table of Contents

Introduction

In October 2016, a distributed denial of service (DDoS) attack by a vast collection of small, cheap Internet-connected devices, which collectively came to be known as the Mirai botnet,[1] paralyzed Internet servers run by a tech firm called Dyn. That, in and of itself, might not have been newsworthy, but the results certainly were given that Dyn managed (and continues to operate) critical Internet infrastructure, access to a number of important Internet services was slowed or stopped for much of the eastern United States. The Mirai botnet was so successful, and noteworthy, because it took advantage of security vulnerabilities in 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.[2] Initially, some thought that the attack was politically motivated, but investigators determined that, in fact, it was not a shadowy group or nation state behind the botnet—they were three college students, trying to get an edge on the *Minecraft* computer game.[3] "'*They didn't realize the power they were unleashing,*'" according FBI agent Bill Walton. "*This was the Manhattan Project*."[4]

There is a great deal of buzz surrounding IoT devices. The rise of "smart products" such as Internet-enabled refrigerators and self-driving cars holds the promise to revolutionize business

---

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

** Harvard University, retired

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

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

[3] Ben Bours, *How a Dorm Room Minecraft Sam Brought Down the Internet*, WIRED (Dec. 13, 2017), https://www.wired.com/story/mirai-botnet-minecraft-scam-brought-down-the-internet/.

[4] *Id*.

and society.[5] But the vast majority of IoT devices are far smaller and cheaper—security cameras, baby monitors, kids toys and the like along with building controls, including light bulbs—"*hungry silicon cockroaches*" as Mike O'Dell, CTO of one of the first big Internet service providers put it.[6] To substantiate the coming wave, Samsung has announced that *all* of its products would be connected to the Internet by 2020.[7] Yet it is an open question whether security can or will scale along with this increasingly crowded field, or whether a combination of perverse incentives, increasing complexity, new problems, and new impacts of old problems like "technical debt" amassing from products being rushed to market, or simple ignorance of security fundamentals, will derail progress and exacerbate prevalent cyber insecurity.[8]

The Mirai botnet episode highlights the complexities in managing the multi-faceted cyber threat facing the public and private sectors. IoT botnets are concerning given that they provide non-state actors—including cybercriminals, politically motivated hacktivists, kids playing around, and nation states[9]—asymmetric capabilities that can be used to target intellectual property and critical infrastructure. An array of public-private partnerships—such as the National Institute for Standards and Technology (NIST) Cybersecurity Framework—efforts by civil society, such as the Consumer Reports Digital Standard, and national governments, such as the UK's Cyber Essentials Plus Certificate, are all being pursued to help harden the Internet of Everything. But will they be enough?

---

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

[6] *See* Mike O'Dell, *Why the Future of the Internet is not Multimedia*, Multimedia Seminar Feb. 26, 1997, https://people.eecs.berkeley.edu/~fox/summaries/conferences/odell.html.

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

[8] This is an industry term for the legacy costs of rolling out new products without first improving security. The Technical Debt Community, http://www.ontechnicaldebt.com/ (last visited Aug. 6, 2015).

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

This Article focuses on cybersecurity standards set by industry, national governments, and by international organizations, to make networks and network-connected devices more secure against the hackers in general and, in particular, against politically-motivated attacks by foreign governments or their proxies. We investigate contemporary approaches to IoT security through an in-depth comparative case study focusing on the European Union and the United States. Particular attention is paid to the impact of the General Data Protection Regulation (GDPR) and the Network Information Security (NIS) Directive in the EU, and influence of the National Institute for Standards and Technology (NIST) Cybersecurity Framework, and other leading standards, on IoT security with a focus on mitigating the risk of politically motivated attacks. We analyze transatlantic reform proposals—including the U.S. Internet of Things (IoT) Cybersecurity Improvement Act of 2017 and the potential for a dedicated NIST Framework for IoT security given the international success of the NIST CSF—and argue for a polycentric approach to boosting IoT securing across both jurisdictions by applying lessons from major Internet governance debates.

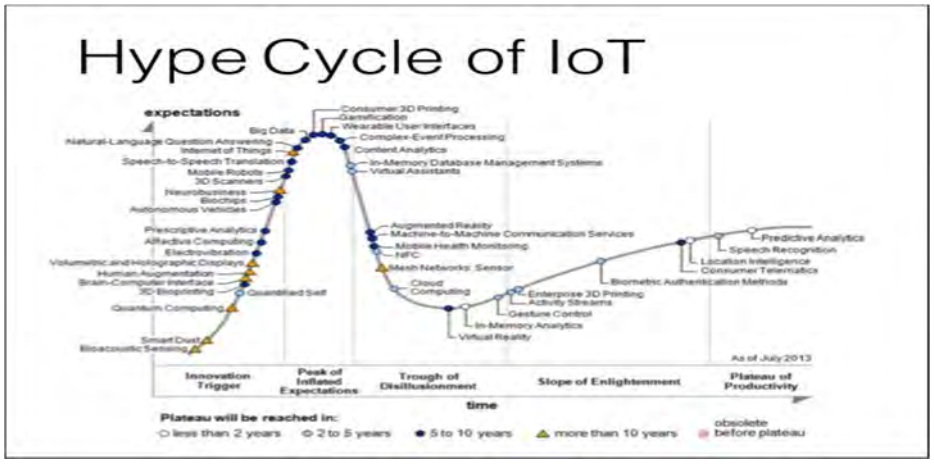
1. Welcome to the Internet of Everything

Although there are differing accounts as to the origin story of the term "Internet of Things," most accounts point to Kevin Ashton coining it in the form of a title for a 1999 presentation for Proctor & Gamble.[10] From those humble beginnings, which included a heavy emphasis on the applicability of Radio Frequency Identification (RFID) technology, which Ashton also had a hand in creating, has come a global effort to make our technology, businesses,

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

and even our bodies, smart.[11] Wherever it came from, the term IoT today now enjoys widespread use in both technology and policy circles, as well as in popular culture.[12] But, in fact, it includes a constellation of devices and technologies with built-in wireless connectivity that "*can be monitored, controlled[,] and linked*"[13] together, as is exemplified in Figure 1.

Figure 1: Gartnet IoT 'Hype Cycle'



As more and more devices – not just computers and smartphones, but thermostats and baby monitors, wristwatches, lightbulbs, doorbells, and even devices implanted in our own bodies – are connected to the Internet, the growing scale of the threat from hackers can easily get lost in the excitement of lower costs and smarter tech.[14] Indeed, smart devices, purchased for

[11] *See, e.g.*, Meghan Neal, *The Internet of Bodies is Coming, and You Could Get Hacked*, MOTHERBOARD (Mar. 13, 2014), https://motherboard.vice.com/en_us/article/gvyqgm/the-internet-of-bodies-is-coming-and-you-could-get-hacked.

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

[13] Bonnie Cha, *A Beginner's Guide to Understanding the Internet of Things*, RECODE (Jan. 15, 2015), https://www.recode.net/2015/1/15/11557782/a-beginners-guide-to-understanding-the-internet-of-things.

[14] *See* Aaron Tilley, *How Hackers Could Use A Nest Thermostat As An Entry Point Into Your Home*, FORBES (Mar. 6, 2015), https://www.forbes.com/sites/aarontilley/2015/03/06/nest-thermostat-hack-home-network/#235d0d693986; Carl Franzen, How to Find a Hack-Proof Baby Monitor, Offspring (Aug. 4, 2017), https://offspring.lifehacker.com/how-to-find-a-hack-proof-baby-monitor-1797534985; Charlie Osborne, *Smartwatch Security Fails to Impress: Top Devices Vulnerable to Cyberattack*, ZDNET (July 22, 2015), http://www.zdnet.com/article/smartwatch-security-fails-to-impress-top-devices-vulnerable-to-cyberattack/; John Markoff, *Why Light Bulbs May B the Next Hacker Target*, N.Y. TIMES (Nov. 3, 2016), https://www.nytimes.com/2016/11/03/technology/why-light-bulbs-may-be-the-next-hacker-target.html?_r=0;

their convenience, are increasingly being used by domestic abusers as a means to harass, monitor, and control their victims.[15] Yet, for all the press that the IoT has received, it remains a topic little understood or appreciated by the public. One 2014 survey, for example, found that fully 87% of respondents had never even heard of the "Internet of Things."[16] And for those who are in the trenches, it is not uncommon for 'cyber fatigue' to set in. Jim Lewis of the Center for Strategic and International Studies, for example, has said, "*Right now we have a faith-based approach to cybersecurity, in that we pray every night that nothing bad will happen.*"[17] In short, managing the growth of the Internet of Everything impacts a diverse set of interests: U.S. national and international security; the competitiveness of firms; global sustainable development; trust in democratic processes; and safeguarding civil rights and liberties in the digital age. How did we get here?

1.1 Historical Development

The notion of deploying, and leveraging the power of, smart devices began long before 1999. Such "intelligent" devices were envisioned even in the 1950s and 1960s. This trend continued during the creation of ARPANET, an undertaking that eventually became what we refer to as the Internet,[18] under the heading of "pervasive computing."[19]

---

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

[16] *See* Chris Merriman, *87 Percent of Consumers Haven't Heard of the Internet of Things*, INQUIRER (Aug. 22, 2014), https://www.theinquirer.net/inquirer/news/2361672/87-percent-of-consumers-havent-heard-of-the-internet-of-things.

[17] Ken Dilanian, *Privacy Group Sues to Get Records About NSA-Google Relationship*, L.A. TIMES (Sept. 14, 2010), http://www.latimes.com/business/la-fi-nsa-google-20100914,0,5669294.story.

[18] 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 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).

[19] Fenn & LeHong, *supra* note 12.

For example, in the early 1980s researchers at Carnegie-Mellon University deployed sensors and switches in a vending machine allowing them to count the number of bottles present and check their temperature.[20] Around the same time, students at MIT deployed a server that could tell you which bathrooms were available.[21] By the 1990s, despite the rapid scaling of the Internet infrastructure, dial-up Internet connectivity with relatively slow connection speeds held back the growth of IoT applications.

The potential of IoT tech was arguably only realized since 2010,[22] the result of the confluence of at least three factors: (1) the widespread availability of always-on high-speed Internet connectivity in many parts of the world; (2) faster computational capabilities permitting the real-time analysis of Big Data; and (3) economies of scale lowering the cost of sensors and chips to manufacturers.[23] However, the rapid rollout of IoT technologies has not been accompanied by any mitigation of the array of technical vulnerabilities across these devices, which are introduced next.

1.2 Technical Vulnerabilities and Use Cases

As has often been observed, the Internet was not designed with security in mind.[24] Access to the early ARPANET was restricted to government-funded researchers and, even after

[20] *See* Press, *supra*, at 18. *See also The Internet of Things: Groundbreaking Tech with Security Risks*, WELIVESEC. (Oct. 29, 2015), 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.").

[21] https://news.ycombinator.com/item?id=7621384

[22] 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/.

[23] *See* Jim Chase, *The Evolution of the Internet of Things*, TX. INSTRUMENTS (2013), www.ti.com/lit/ml/swrb028/swrb028.pdf; Scott J. Shackelford et al., *When Toasters Attack: Enhancing the 'Security of Things' through Polycentric Governance*, 2017 UNIV. ILL. L. REV. 415 (2017).

[24] Craig Timberg, *A Flaw in the Design*, WASH. POST (May 30, 2015), https://www.washingtonpost.com/sf/business/2015/05/30/net-of-insecurity-part-1/?noredirect=on&utm_term=.a1070f278002.

more than a decade, less than a thousand computers were connected to it.[25] With a limited and controlled set of users' security was not considered an issue to be worried about. Thus, the underlying architecture and protocols of the Internet do not have security "built-in."[26]

Because the network does not provide any kind of security protection, security is left to the devices connected to the network. Too many Internet device or software vendors have been slow to understand that it is the vendor's job to provide security in the systems they sell. For example, it was not until early 2002 that Microsoft, the primary vendor of operating system software for Internet-connected devices, made security a primary goal.[27] To this day, far too many medical devices have inadequate security,[28] industrial controllers are often vulnerable because vendors assumed they would be on isolated networks, not the Internet.[29] IoT toys and devices such as security cameras and baby monitors, have fixed and unchangeable access passwords which, when discovered (not if) open the devices to exploitation.[30] This is now easily done by making use of websites such as Shodan, which can allow anyone (hackers and defenders alike) to search for IoT devices connected to the Internet.[31] Many IoT devices are built using embedded computing modules that were programmed by component manufacturers who,

---

[25] Robert Zakon, *Hobbes' Internet Timeline 25*, 2018, https://www.zakon.org/robert/internet/timeline/

[26] *See* Timberg, *supra* note 23.

[27] Bill Gates, *Trustworthy Computing*, Jan. 15, 2002, https://www.wied.com/2002/01/bill-gates-trustworthy-computing/.

[28] Lily Hay Newman, *Medical Devices are the Next Security Nightmare*, WIRED (Mar. 2, 2017), https://www.wired.com/2017/03/medical-devices-next-security-nightmare/; Scott J. Shackelford et al., *Securing the Internet of Healthcare*, __ MINNESOTA J. OF LAW, SCI. & TECH. __ (forthcoming 2018).

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

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

[31] *See* Showdan, https://www.shodan.io/ (last visited July 1, 2018).

demonstrably, have little to no security expertise.[32] Regrettably, the U.S. government has been slow to help correct this market failure.

2. U.S. Case Study

The United States, long a pioneer in Internet technologies and their regulation, has increasingly focused on the promise and peril of IoT technologies, including the ways in which they could be leveraged for politically motivated hacking. This section unpacks the current U.S. regulatory framework pertaining to IoT devices before moving to analyze reform efforts—namely the IoT Cybersecurity Improvement Act of 2017. We then discuss the utility of cybersecurity frameworks and standards, focusing on those published by NIST and Consumer Reports, to better understand whether these bottom-up efforts will be sufficient at helping to fill prevailing governance gaps.

2.1 Current Regulatory Landscape

The U.S. has favored a generally voluntary, sector-specific or topic-specific approach to both cybersecurity and data privacy, unlike the more mandatory and comprehensive approach favored in the European Union, discussed in Part 3, as may be seen in the General Data Protection Regulation (GDPR), which came into force in May 2018.[33] In short, not all private data is created equal in the United States, it matters if it is health or financial data, or your IP address or Internet searches. The latter, for example, are safeguarded by GDPR as personal data for European Union citizens, but U.S. citizens

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

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

do not enjoy similar protections.[34] Similarly, cybersecurity regulation—particularly in the IoT context—includes a patchwork of federal and state laws and policies, which are summarized below and compared in Part 3 to the European Union.

Due to the breadth and complexity inherent in the field, federal cybersecurity law is largely unprepared to mitigate security problems arising in the IoT context.[35] Governance gaps remain common, despite the best efforts by groups such as the Federal Trade Commission (FTC), which encourages, but does not require, firms to:

1. 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.[36]

In sum, the FTC recommends "*tackling cybersecurity 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*

[34] *See What is Personal Data?*, EU GDPR COMPLIANT, https://eugdprcompliant.com/personal-data/ (last visited May 29, 2018).

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

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

ultimately secure data deletion."[37] These suggestions are in line with both the 2014 NIST Cybersecurity Framework and the 2015 NIST IoT Framework discussed next.

The FTC actually has authority, granted in Section 5 of the Federal Trade Commission Act establishing the FTC, to create rules to block "*unfair or deceptive acts or practices*" on the part of companies doing business in the United States.[38] The FTC has interpreted this authority in a way that permits it to level penalties against companies whose cybersecurity is not up to par if the company implies or advertises that they use certain cybersecurity practices, or if they operate in at-risk critical infrastructure sectors such as healthcare. The FTC interpretation was upheld by the U.S. Court of Appeals for the Third Circuit in 2015 in *FTC v. Wyndham Worldwide*.[39] However, based on a recent case, *LabMD Inc. v. Federal Trade Commission*, the FTC may need to become more specific in the cybersecurity standards it requires of businesses. In essence, the Eleventh U.S. Circuit Court of Appeals ruled in June 2018 that, since the FTC had not provided specific cybersecurity standards defining reasonableness for LabMD, a now bankrupt cancer-screening company, the FTC's order was illegal.[40]

While not challenging the FTC's authority to police cybersecurity, the court did significantly tighten the grounds over which the FTC could initiative investigations and levy fines and settlement orders. Specifically, the underlying data breach must violate some specific law such as the Health Insurance Portability and Accountability Act of

---

[37] *See 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/.

[38] FTC, *A Brief Overview of the Federal Trade Commission's Investigative and Law Enforcement Authority*, FTC (2008), https://www.ftc.gov/about-ftc/what-we-do/enforcement-authority.

[39] W. Reece Hirsch et al., *Third Circuit Sides with FTC in Data Security with Wyndham*, NAT'L L. REV. (Sept. 8, 2015), https://www.natlawreview.com/article/third-circuit-sides-ftc-data-security-dispute-wyndham.

[40] Allison Frankel, *There's a Big Problem for the FTC Lurking in the 11th Circuit's LabMD Data-Security Ruling*, 2018, https://www.reuters.com/article/us-otc-labmd/theres-a-big-problem-for-the-ftc-lurking-in-11th-circuits-labmd-data-security-ruling-idUSKCN1J32S2

1996 (HIPPA).[41] Thus, the FCT cannot penalize a company for the release of data causing a substantial consumer injury if it is not subject to an existing law. The Eleventh Circuit did not address whether the FTC's use of the negligence tort sufficed in this case. The upside is that there seems to be a growing circuit split over the FTC's cybersecurity oversight powers focusing on the Third and Eleventh Circuits, which could result in a state of affairs (unless Congress intervenes) in which no U.S. government agency can penalize a company simply for having lax cybersecurity unless it runs afoul of existing constitutional or sector-specific statutory prohibitions.[42]

2.2 Analyzing the NIST CSF

Frustrated with the lack of Congressional action on cybersecurity, President Obama announced his desire in 2013 for the U.S. government to partner with industry and develop a framework comprised of private-sector cybersecurity best practices that would help guide firms of all sizes, but particularly critical infrastructure operators.[43] The result was the first 2014 NIST Cybersecurity Framework (NIST CSF), which is critical since—even though it has been criticized as leading to a reactive stance[44]—it is spurring the development of a baseline standard of cybersecurity due diligence in the United States.[45] In particular, the NIST CSF harmonizes industry best practices to

---

[41] *Id*.

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

[43] *See* NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, IMPROVING CRITICAL INFRASTRUCTURE CYBERSECURITY EXECUTIVE ORDER 13636: PRELIMINARY CYBERSECURITY FRAMEWORK 1 (2013), *available at* http://www.nist.gov/itl/upload/preliminary-cybersecurity-framework.pdf.

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

[45] *See, e.g.*, Scott J. Shackelford et al., *Toward a Global Standard of Cybersecurity Care?: Exploring the Implications of the 2014 Cybersecurity Framework on Shaping Reasonable National and International Cybersecurity Practices*, 50 TEX. J. INT'L L. 287 (2015); Scott J. Shackelford, Scott Russell, & Andreas Kuehn,

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 NIST CSF replacing organizations' existing security policies, NIST has intended 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*."[46] Although the NIST CSF was only published in 2014,[47] 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 CSF*."[48] Over time, the NIST CSF not only has the potential to shape a standard of care for domestic critical infrastructure organizations but also could help to harmonize global cybersecurity best practices for the private sector writ large given active NIST collaborations with more than twenty nations including the United Kingdom, Japan, Korea, Estonia, Israel, and Germany.[49] This progress has continued with the publication of Version 1.1 of the NIST CSF in April 2018, which, as Secretary of Commerce Wilbur Ross has argued "*should be every company's first line of defense*."[50] The new version

---

Defining Cybersecurity Due Diligence Under International Law: Lessons from the Public and Private Sectors, 17 CHI. J. INT'L L. 1 (2016).

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

[47] *See Framework for Improving Critical Infrastructure*, NIST (Apr. 2015), http://www.nist.gov/cyberframework/upload/cybersecurity_framework_bsi_2015-04-08.pdf (noting that "To allow for adoption, Framework version 2.0 is not planned for the near term.").

[48] *Why the NIST Cybersecurity Framework Isn't Really Voluntary*, INFO. SEC. BLOG (Feb. 25, 2014), http://www.pivotpointsecurity.com/risky-business/nist-cybersecurity-framework.

[49] 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-thegovernment-to-sue-companies-for-getting-hacked/?wpmm=1&wpisrc=nl_headlines.

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

boasts significant improvements, including with regards to authentication, supply chain cybersecurity, and vulnerability disclosure, though it is still best considered a cybersecurity floor rather than a ceiling.[51] It does not, fore example, focus on IoT issues in particular, which is an area that many would like NIST to address in more detail.

2.3 Case for a NIST IoT Framework

Beyond the general NIST CSF, NIST has also released another Framework focusing on IoT issues entitled the "*Framework for Cyber-Physical Systems*" ("NIST IoT Framework") in September 2015.[52] 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*."[53] 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*."[54] Similar to the 2014 NIST CSF, the 2015 NIST IoT Framework was developed through a multi-stakeholder process 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*."[55] As with the NIST CSF, the 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*

[51] *See id*.

[52] *See, e.g.*, *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/.

[53] HOGAN LOVELLS, *supra* note 52.

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

[55] *Id*.

of CPS."[56] To aid in these goals, the NIST IoT Framework identifies CPS domains as well as analyzing and addressing cross-cutting concerns.[57] Although both the 2014 NIST CSF 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,[58] some argue that the existing NIST IoT Framework is not specific (or user-friendly) enough to make the same impact on IoT as the NIST CSF has had on critical infrastructure protection.

2.4 Unpacking the Proposed IoT Cybersecurity Improvement Act of 2017

Another path forward is to rely more specifically on Congressional regulation to do what, thus far, standards have failed to deliver. Senators Mark Warner, Cory Gardner, Ron Wyden, and Steve Daines introduced *the Internet of Things Cybersecurity Act of 2017* with this aim in mind. In brief, the legislation would require vendors who sell products to the U.S. government to: (1) ensure that their devices "*are patchable*," (2) that they do not "*contain known vulnerabilities*," that they "*rely on standard protocols*," and (4) they "*don't contain hard-coded passwords*."[59] However, the bill does not take a one-sized-fits-all to regulating an area as vast as IoT. Indeed, the authors provide a path forward whereby, if industry provides "*equivalent, or more rigorous, device security requirements*" then they may be utilized in lieu of the foregoing.[60] The legislative effort has a long list of proponents from Bruce Schneier and Professor Jonathan Zittrain to leading voices from Symantec and the Center for Democracy and Technology,[61] but also has its

[56] NIST IoT Framework, *supra* note 52, at xii.
[57] *Id*. at xiii.
[58] *See* Shackelford et al., *supra* note 45.
[59] IoT Cyber Bill Factsheet, https://www.warner.senate.gov/public/_cache/files/8/6/861d66b8-93bf-4c93-84d0-6bea67235047/8061BCEEBF4300EC702B4E894247D0E0.iot-cybesecurity-improvement-act---fact-sheet.pdf.
[60] *Id*.
[61] *Id*.

share of critics.[62] Overall, though, the bill only has a thirteen percent chance of becoming law as of June 2018, according to Skopos Labs,[63] leading one to consider alternatives.

2.5 Role of the Consumer Reports Digital Standard

Instead of black letter regulation, many, particularly in industry, prefer self-regulation with the flexibility "*to adapt to rapid technological progress*"[64] Such self-regulation has the capacity to adapt better and faster than black letter law to rapidly changing technological and social forces. It can also be efficient and cost-effective than command and control-style regulation,[65] though it is not a panacea, which is why communal self-governance is but one component of polycentric governance discussed further in Part 3.[66] Indeed, the benefits of self-regulation are not absolute and depend on certain community characteristics. One organization that is trying to create such a community is *Consumer Reports*. Specifically, in March 2017 *Consumer Reports* launched its Digital Standard, which is designed "*to measure the privacy and security of products, apps, and services will put consumers in the driver's seat as the digital marketplace evolves*."[67] Once it fully matures, the Digital Standard will empower consumers to be able to select products—including in the IoT context—that meet rigorous privacy and security

---

[62] *See New Bill Seeks Basic IoT Security Standards*, Krebs on Sec. (Aug. 1, 2017), https://krebsonsecurity.com/2017/08/new-bill-seeks-basic-iot-security-standards/.

[63] *See S. 1691: Internet of Things (IoT) Cybersecurity Improvement Act of 2017 Track S. 1691*, https://www.govtrack.us/congress/bills/115/s1691 (last visited June 4, 2018).

[64] MONROE E. PRICE & STEFAN G. VERHULST, SELF-REGULATION AND THE INTERNET 21 (2005). According to Notre Dame Professor Don Howard, different online communities "have a complicated topology and geography, with overlap, hierarchy, varying degrees of mutual isolation and mutual interaction. There are also communities of corporations or corporate persons, gangs of thieves, and . . . 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.

[65] *See* PRICE & VERHULST, *supra* note 64, at 21–22.

[66] Elinor Ostrom, *Polycentric Systems as One Approach for Solving Collective-Action Problems* 2–3 (Ind. Univ. Workshop in Political Theory and Policy Analysis, Working Paper Series No. 08-6, 2008).

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

requirements. But, since *Consumer Reports* is not a regulatory organization, vendors will still be legally able to sell products that do not meet the Standard. Over time, the Standard holds the promise of helping the market function more efficiently by rewarding those firms that take cybersecurity and data privacy seriously, and penalizing those that do not through lower scores and, as a result, less revenue. Already, these efforts are having an impact, such as when it helped expose privacy risks in the pregnancy and fertility app Glow.[68] As the Digital Standard is continually refined, and globalized, it will likely further impact the trajectory and rate of global IoT privacy and security standards.[69]

3. E.U. Case Study

The European Union has long taken a distinct and much more mandatory and comprehensive approach to both cybersecurity and information privacy from the more sector-specific regime preferred in the United States.[70] This fact may be seen in 2018 with the passage of the *Network Information Security (NIS) Directive*, and the enactment of the *General Data Protection Regulation (GDPR)*, which are explored in this section. This approach is not without its critics, such as those who are concerned about over-centralization,[71] but it is equally true that

[68] *Glow Pregnancy App Exposed Women to Privacy Threats, Consumer Reports Finds*, CONSUMER REPORTS (July 28, 2016), https://www.consumerreports.org/mobile-security-software/glow-pregnancy-app-exposed-women-to-privacy-threats/.

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

[70] *See, e.g.*, Scott J. Shackelford, *Seeking a Safe Harbor in a Widening Sea: Unpacking the EJC's Schrems Decision and What it Means for Transatlantic Relations*, __ SETON HALL J. OF DIPLOMACY & INT'L REL. __ (forthcoming 2018).

[71] Response to EU Cybersecurity Strategy and proposed Directive on Network and Information Security (NIS), EurActiv Press Release (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

these efforts have made the EU a global leader in information governance best practices. Moreover, it should also be noted that transatlantic approaches to how organizations should manage their cyber risk are converging, with a coalescing around the language of risk management, as may be seen by the EU's *Network Information Security Public-Private Platform* (NIS Platform), which specifically adopts the NIST core – identify, protect, detect, respond, recover – as the industry-standard EU approach for cybersecurity risk management.[72] The 2013 EU Cybersecurity Strategy introduced the NIS Directive's goal to "*facilitate exchange of best practices*," enhance "*risk management practices and information sharing*"[73] through the establishment of the NIS Platform.[74] This Platform helped collect "*existing risk management standards and best practices*" [75] that organizations "*can use and tailor to their own approach to risk management*."[76]

As with cybersecurity and information privacy generally, the EU has long been engaged with IoT issues in particular. As one example, in 2014 the European Commission funded a project named COPHER, which had the goal of conducting an "*in-depth analysis of the reality of security in privately held information systems in Europe*."[77] Specifically, CIPHER included an effort to draft a regulatory roadmap with

---

draft Network and Information Security Directive from working hand-in-hand with industry, to top-down, unidirectional reporting obligations and requirements.").

[72] NIS Platform (WG-1) Final Draft 220515, Network and Information Security Risk Management Organizational Structures and Requirements, *available at* 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. For more on this topic, see Scott J. Shackelford, Scott Russell, & Jeffrey Haut, *Bottoms Up: A Comparison of "Voluntary" Cybersecurity Frameworks*, 16 UNIV. CAL. DAVIS BUS. L.J. 217 (2016).

[73] A CYBER SECURITY FRAMEWORK FOR EUROPE, EUR. COMM'N (last updated on Aug. 5, 2014), http://cordis.europa.eu/news/rcn/121360_en.html.

[74] ENISA, NETWORK AND INFORMATION SECURITY RISK MANAGEMENT ORGANIZATIONAL STRUCTURES AND REQUIREMENTS 14 (2015), https://resilience.enisa.europa.eu/nis-platform/shareddocuments/5th-plenary-meeting/chapter-1-nis-risk-management-organisational-structures-andrequirements-v2.

[75] *Id.* at 4.

[76] *Id*. at 14.

[77] A CYBER SECURITY FRAMEWORK FOR EUROPE, *supra* note 73.

recommendations for policymakers that included IoT.[78] The European Commission has also founded the *Alliance for Internet of Things Innovation*, which has been tasked with developing a large-scale framework specifically addressing issues within IoT.[79] The group has also engaged internationally, welcoming delegations from around the world to discuss IoT governance,[80] reinforcing the EU's place as a key hub for cybersecurity and privacy governance. Finally, in late 2015 the European Commission launched *Horizon 2020*, which included goals for smart cities and IoT deployment.[81] 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 an array of consumer products including clothes, fabrics, patches, watches and other body-mounted devices*."[82] These goals demonstrate how the EU is planning to secure the full gambit of IoT devices.[83]

3.1 GDPR's Application to IoT Security

A key aspect for how the EU will shape IoT governance is through the GDPR, which is an extension of its long push to create a *Digital Single Market* (DSM). Although most of the press coverage of the GDPR has focused on its privacy protection regulations and the potentially very large penalties that can be imposed for not following the data privacy rules, an important goal of the GDPR is to tear down, to the extent feasible,

[78] *Id*.

[79] Alliance for Internet of Things Innovation, Working Group 3 Report, IoT LSP Standard Framework Concepts, Release 2.0, AIOTI WG03 – loT Standardisation (2015).

[80] *See* AIOTI News, https://aioti.eu/news/ (last visited June 5, 2018).

[81] 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.

[82] *Id*.

[83] *Id*. at 93.

remaining regulatory walls between the EU Member States and move toward a single EU market.[84] Similar to the NIST CSF, which "*relies on a variety of existing standards, guidelines, and practices to enable critical infrastructure providers to achieve resilience,*"[85] the DSM synthesizes initiatives on security and data protection.[86] 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*" that are issues critical to boosting the Security of Things.[87]

Building from this foundation, GDPR is an expansive regulatory regime with a wide array of requirements on covered firms ranging from ensuring data portability and consent to mandating that firms disclose a data breach within 72-hours of it becoming aware of the incident and then conducting a post mortem to ensure that a similar scenario will not recur.[88] As groundbreaking as these regulations are, though, they were not drafted with IoT in mind, despite a 2017 finding by the European Union Agency for Network and Information Security (ENISA) "*that there were no 'legal guidelines for IoT device and service trust.' Nor any 'level zero defined for the security and privacy of connected and smart devices.'*"[89] Further, European-level regulation is slow, and a blunt

---

[84] EUR. COMM'N, COMMISSION PRIORITY, DIGITAL SINGLE MARKET, BRINGING DOWN BARRIERS TO UNLOCK ONLINE OPPORTUNITIES DIGITAL SINGLE MARKET, http://ec.europa.eu/priorities/digital-single-market/index_en.htm.

[85] *See Framework for Improving Critical Infrastructure*, NIST, at 4 (Apr. 2015), http://www.nist.gov/cyberframework/upload/cybersecurity_framework_bsi_2015-04-08.pdf (noting that "To allow for adoption, Framework version 2.0 is not planned for the near term.").

[86] DSM, *supra* note 84.

[87] EUR. COMM'N, AN ENVIRONMENT WHERE DIGITAL NETWORKS AND SERVICES CAN PROSPER, http://ec.europa.eu/priorities/digital-single-market/environment/index_en.htm (last visited Dec. 16, 2017).

[88] *See, e.g.*, Top Ten Operational Impacts of the GDPR, Int'l Assoc. Privacy Prof., https://iapp.org/resources/article/top-10-operational-impacts-of-the-gdpr/ (last visited June 5, 2018).

[89] Scott Gordon, *Will we Get a GDPR for the IOT?*, SC MAG. (Apr. 26, 2018), https://www.scmagazineuk.com/will-we-get-a-gdpr-for-the-iot/article/758037/.

instrument – GDPR, as one example, took more than four years to be adopted after having been proposed in 2012.[90]

Directives such as the NIS Directive have the benefit of providing more freedom to nations to craft solutions to common problems, such as the need for more robust critical infrastructure protection, but this can similarly be a cumbersome process.[91] 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 policymakers 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.*"[92] Many commentators argue that this "*type of active industry 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 is one that other nations are seeking to emulate*."[93] For example, the French government is considering mandating liability for security lapses on the part of IoT manufacturers.[94] The UK has also been active in developing cybersecurity standards, which is the illustrative example we turn to next.

---

[90] *Id*.

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

[92] Cybersecurity Framework Frequently Asked Questions, http://www.nist.gov/cyberframework/cybersecurity-framework-faqs.cfm (last visited Sept. 21, 2015) ("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.").

[93] Shackelford, Russell, & Haut, *supra* note 72.

[94] Gordon, *supra* note 89.

3.2 UK's Cyber Essential Plus Certificate

The UK's cybersecurity policymaking efforts, much like the United States, have focused on developing voluntary standards. The UK Cyber Security Strategy is the overarching cybersecurity policy promulgated by the British government.[95] The 2011 Strategy focused on tackling cybercrime, increasing overall resilience to cyber attacks, and encouraging the development of industry-led cybersecurity norms.[96] However, the 2011 Strategy did not specifically address cybersecurity awareness-raising for individuals and businesses that were not identified as components of the UK's critical infrastructure.[97]

The 2011 Strategy was extended in June 2014 when the GCHQ, BIS, and Cabinet Office created *Cyber Essentials*, a best practices certification program backed by the British government, which was supported by industry leaders.[98] The Cyber Essentials program's primary purpose is to "*incentivize widespread adoption of basic security controls that will help to protect organizations against the commonest kind of internet attack*."[99] The scheme is mandatory for all UK government contractors handling PII,[100] and has two schemes*: Cyber Essentials* and *Cyber Essentials Plus*.[101] Cyber Essentials' requirements involve self-certification for basic organizational cyber hygiene practices,

---

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

[96] *Id.*

[97] *Id.*

[98] *Id.* at 7.

[99] *Id.*

[100] Cabinet Office, Policy Paper, "2010 to 2015 Government Policy: Cyber Security" (updated May 8, 2015), https://www.gov.uk/government/publications/2010-to-2015-government-policy-cyber-security/2010-to-2015-government-policy-cyber-security#appendix-7-working-with-industry-on-minimum-standards-and-principles.

[101] UK DEPT. BUS., INNOVATION & SKILLS, CYBER ESSENTIALS SCHEME SUMMARY (June 2014), http://www.cyberstreetwise.com/cyberessentials/files/scheme-summary.pdf.

such as firewalls, secured configuration, user access control, and patch management.[102] The Cyber Essentials Assurance Framework is intended for supplementation of existing organizational approaches to risk management.[103] Specifically, the Cyber Essentials certification calls on businesses to follow the British government's Ten Steps to Cyber Security, which is reminiscent of the FTC's Guide for Business.[104] Perhaps the most important recent development, though, came in January 2015 with the addition of the *Advice Sheets* ("Advice Sheets") to the 10 Steps to Cyber Security program.[105] The Advice Sheets set out *"[the] actions and measures . . . [that represent] a good foundation for effective information risk management . . . to safeguard a company's most valuable assets*"[106] while acknowledging that the degree of implementation may be variable, depending upon the cyber risks to a given organization.[107] The more recent 2016 UK National Cybersecurity Strategy moves forward on some of these issues, but only references IoT issues in passing.[108] Still, the Cyber Essentials program has produced a following, and have helped businesses across the country market cybersecurity as a competitive advantage, instead of merely a cost of doing business.[109]

4. Policy Implications

---

[102] *Id*.

[103] *Id*.

[104] UK DEPT. BUS., INNOVATION & SKILLS, CYBERSECURITY GUIDANCE FOR BUSINESS (Jan. 16, 2015), https://www.gov.uk/government/publications/cyber-risk-management-a-board-level-responsibility.

[105] U.K. CABINET OFFICE, TEN STEPS TO CYBER SECURITY (2012), https://www.gov.uk/government/publications/10-steps-to-cyber-security-advice-sheets.

[106] *Id*.

[107] *Id.*

[108] NATIONAL CYBER SECURITY STRATEGY 2016-2021, at 40, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf.

[109] *See Cyber Essentials*, NAT'L CYBER SEC. CTR., https://www.cyberessentials.ncsc.gov.uk/getting-certified/ (last visited June 5, 2018).

4.1 Need for a Polycentric Approach to Secure Critical Infrastructure in the IoT Context

There are many ways to conceptualize cybersecurity policy, 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[110] that has been championed by numerous scholars including Nobel Laureate Elinor Ostrom and Professor Vincent Ostrom, which challenges orthodoxy in part by demonstrating the benefits of self-organization and networking regulations "*at multiple scale*s."[111] 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*"[112] 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*."[113] 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

[110] Michael D. McGinnis, *An Introduction to IAD and the Language of the Ostrom Workshop: A Simple Guide to a Complex Framework*, 39(1) POL'Y STUD. J. 163, 171–72 (Feb. 2011), http://php.indiana.edu/~mcginnis/iad_guide.pdf (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.").

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

[112] Elinor Ostrom, *A Polycentric Approach for Coping with Climate Change* 35 (World Bank, Policy Research Working Paper No. 5095, 2009), http://www.iadb.org/intal/intalcdi/pe/2009/04268.pdf.

[113] Robert O. Keohane & David G. Victor, *The Regime Complex for Climate Change* 9 PERSP. ON POL. 7, 9 (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").

network effects that could, in time, result in the emergence of a norm cascade improving the Security of Things.[114]

One example of a successful public-private polycentric collaboration is the NIST CSF, which, as has been noted, is now going global. The success of such frameworks, civil society efforts like the Consumer Reports Digital Standard, and regional regimes like GDPR, is part and parcel of the literature on polycentric governance. However, it is important to note that not all polycentric systems are guaranteed to be successful. Disadvantages, for example, can include gridlock and a lack of defined hierarchy.[115] The Ostrom Design Principles can help predict the institutional success of given interventions.[116] Still, the literature remains immature, as does the current state of IoT governance. In fact, the Information Systems Audit and Control Association (ISACA)[117] 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."[118] What lessons can be learned, then, from how the Internet itself evolved and applied to IoT?

4.2 Looking Back: Applying Lessons from Internet Governance

The Internet has succeeded rather well in spite of the fact that only period of time that the Internet had any real governance is before it became the Internet – the pre-Internet ARPANET

---

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

[115] *See* Robert O. Keohane & David G. Victor, *The Regime Complex for Climate Change*, 10 (Harvard Kennedy Sch., Discussion Paper 10-33, 2009) (internal quotation marks omitted), http://belfercenter.ksg.harvard.edu/files/Keohane_Victor_Final_2.pdf.

[116] For more on this topic, see Shackelford et al., *Toasters*, *supra* note 23.

[117] Previously known as **'**Information Systems Audit and Control Association,' http://www.isaca.org/about-isaca/Pages/default.aspx (last visited Dec. 16, 2015).

[118] *Existing Security Standards Do Not Sufficiently Address IoT*, IN SEC. (Oct 2015) http://www.net-security.org/secworld.php?id=18981.

(before 1983) – and for a few years thereafter. During this time ARPANET, and the overlapping NSFNET, were paid for and operated under contract with the U.S. government.[119] But with the end of the government-run Internet backbone networks in the early 1990s and the rise of independent commercial Internet service providers came the end of an integrated governance structure. Instead, Internet service providers in the United States and elsewhere informally agreed to use the same set of technical standards and formed bilateral contracts (the sinews of polycentric governance) between themselves.[120] Together, these agreements and complementary technical standards are what enabled the Internet to scale to the ubiquity that it enjoys today.

The Internet technical standards are a key part of the Internet's success and the standards did start with U.S. government action. A decade after the first nodes of the ARPANET were interconnected in 1969, ARPA chartered a committee, the Internet Configuration Control Board (ICCB) to "*guide the technical evolution of the Internet Protocol suite*."[121] After several transformations the ICCB evolved into the *Internet Engineering Task Force* (IETF),[122] which is currently the primary technical standards body for the Internet.[123] The technical standards developed or maintained by the IETF are voluntary, the government does not mandate adherence to them but if an ISP or an equipment vendor does not support a core set of technical standards they would not be able to interoperate with the rest of the Internet.

Over the years there have been many attempts to formalize Internet governance, such as granting a greater governance role to the *International Telecommunications Union* (ITU). But, to date, none of these efforts have succeeded, though there have been important milestones along

---

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

[120] Vint Cerf, *The Internet Activities Board* (1990), https://www.ietf.org/rfc/rfc1160.txt.

[121] *Id*.

[122] Internet Engineering Task Force, https://www.ietf.org/.

[123] Scott Bradner, *Internet Engineering Task Force, in* OPEN SOURCES: VOICES FROM THE OPEN SOURCE REVOLUTION 47, 47 (1999).

the way such as the creation of the Internet Governance Forum in 2006 and the U.S. Department of Commerce's decision not renew its contract with the Internet Corporation for Assigned Names and Numbers (ICANN) in 2016.[124] However, taking the IETF as a model would argue that the U.S. voluntary security standards could be a successful path to security for the IoT. But there is a significant difference between the Internet's voluntary technical standards and the voluntary security standards provided by NIST and others: a device that does not correctly implement the Internet technical standards will not be able to operate in the Internet, a strong forcing factor. On the other hand, a device that does not correctly implement security standards will interoperate, even though it a risk to wider Internet ecosystem.

4.3 Looking Ahead: Operationalizing Cybersecurity Due Diligence in the Internet of Everything

At least two strategic paths forward can help firms, and the jurisdictions under which they operate, mitigate cyber risk in the IoT context. The first option is to further refine and operationalize the concept of cybersecurity due diligence. In the private-sector transactional context, cybersecurity due diligence has been defined as "the review of the governance, processes and controls that are used to secure information assets."[125] This increasingly central concept to a variety of business activities as it is used here builds from this definition and may be understood as the corporate, national, and international obligations of both State and non-State actors to help identify and instill cybersecurity best practices and effective governance

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

[125] Tim Ryan & Leonard Navarro, *Cyber Due Diligence: Pre-Transaction Assessments Can Uncover Costly Risks*, KROLL CALL (Jan. 28, 2015), http://blog.kroll.com/2015/cyber-due-diligence-pre-transaction-assessments-can-uncover-costly-risks/.

mechanisms so as to promote cyber peace.[126] Put more simply, due diligence refers to your activities to identify and understand the various risks facing an organization. Cybersecurity due diligence, then, is centered on risk management best practices and obligations that may exist between States, between non-State actors (e.g., private corporations, end-users), and between State and non-State actors,[127] and refers to the international obligations of both State and non-State actors to help identify and instill cybersecurity best practices so as to promote the Security of Things. In so doing, the norm "commits states to ensuring that no actions originating on their territory in times of peace violate the rights of other states."[128] But determining exactly what nations' due diligence obligations are to secure IoT devices and to prosecute or extradite cyber attackers is no simple matter.[129] A key aspect of this effort is effective information sharing, e.g., government intelligence agencies cooperating with one another to detect such attacks and to inform the targets. Without such information, the targets would often not even know if they were under attack, since few sophisticated attacks are detected,[130] and would not know that they needed to strengthen their defences.

However, given the failure of the 2017 UN Group of Government Experts (GGE) negotiations regarding cybersecurity norms including due diligence, another lens through which

---

[126] For a discussion of cyber peace, see Scott J. Shackelford, *The Meaning of Cyber Peace,* NOTRE DAME INST. ADV. STUDY Q. (2013), https://ndias.nd.edu/news-publications/ndias-quarterly/the-meaning-of-cyber-peace/.

[127] An earlier version of this research was previously published as Shackelford, Russell, & Kuehn, *supra* note **Error! Bookmark not defined.**.

[128] Annegret Bendiek, *Due Diligence in Cyberspace: Guidelines for International and European Cyber Policy and Cybersecurity Policy*, SWP RESEARCH PAPER 7 (2016), http://www.swp-berlin.org/fileadmin/contents/products/research_papers/2016RP07_bdk.pdf [hereinafter "*Due Diligence in Cyberspace*"].

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

[130] VERIZON 2018 DATA BREACH INVESTIGATIONS REPORT 40 (2018), https://www.verizonenterprise.com/verizon-insights-lab/dbir/.

to view IoT security is sustainable development. In short, organizations should treat cybersecurity as a matter of corporate social responsibility to safeguard their customers and the public, such as by securing vulnerable IoT devices.[131] It is in corporations own, long-term self-interest (as well as that of national security) to take such a wider view of private-sector risk management practices so as to encompass less traditional factors akin to what companies have done with respect to sustainability. An array of concepts and tools explored in this Article—such as certification schemes and standards—that have grown up in the sustainability space are readily applicable to better managing cyber attacks.[132] In the introduction of *Silent Spring*, Rachel Carson speaks of a once idyllic U.S. town now blighted by a "white granular powder . . ."[133] It was not caused by "witchcraft . . . The people had done it to themselves."[134] That is equally true in sustainability as cybersecurity; we are to blame, and we are the solution.

Conclusion

As the Internet of Everything matures, disparate smart residential and commercial networks will be able to communicate with one another, creating smart (and potentially more resilient) things, cities, and societies. Such an ultimate, macro-level outcome resembles the early days of networking when Cisco used multi-protocol routing to join dissimilar networks that eventually led to the widespread adoption of a common networking standard called the Internet Protocol, which we all rely on today every time we sign online. IoT looks set to follow a similar route, albeit on a larger scale, spanning myriad sectors and industries. In response, polycentric IoT cybersecurity regulations should be adapted and improved to better keep pace with these

[131] *See* Scott J. Shackelford & Amanda N. Craig, *Beyond the New 'Digital Divide': Analyzing the Evolving Role of Governments in Internet Governance and Enhancing Cybersecurity*, 50 STAN. J. INT'L L. 119 (2014).

[132] For more on this topic, see Scott J. Shackelford et al., *Sustainable Cybersecurity: Applying Lessons from the Green Movement to Managing Cyber Attacks*, 2016 UNIV. ILL. L. REV. 1995.

[133] RACHEL CARSON, SILENT SPRING 3 (1962).

[134] *Id*.

changes,[135] particularly with regards to data regulations monitoring private firms and companies that transfer PII.[136] This includes standards—including a NIST IoT-specific effort—along with the Consumer Reports Digital Standard, and the use of corporate governance structures, such as sustainability, and international norms, including due diligence. Such an all-of-the-above polycentric approach is essential to addressing governance gaps in the Internet of Everything. As Professor Elinor Ostrom said, this not a "keep it simple, stupid" response,[137] but a multifaceted one in keeping with the complexity of the crises in Internet governance.

[135] *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.

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

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