Minnesota Journal of Law, Science & Technology

Volume 21 | Issue 1 Article 1

12-21-2019

# Smart Factories, Dumb Policy? Managing Cybersecurity and Data Privacy Risks in the Industrial Internet of Things

Scott J. Shackelford

# Smart Factories, Dumb Policy? Managing Cybersecurity and Data Privacy Risks in the Industrial Internet of Things

**Prof. Scott J. Shackelford* JD, PhD**

ABSTRACT

*Interest is booming in the so-called Internet of Things (IoT). The Industrial Internet of Things (IIoT) is one application of this trend and involves the use of smart technologies in a manufacturing context. Even though these applications hold the promise to revolutionize manufacturing, there are a number of outstanding cybersecurity and data privacy issues impacting the realization of the myriad benefits promised by IIoT proponents. This article analyzes some of these pressing issues, focusing on: (1) critical infrastructure protection and cybersecurity due diligence, (2) trends in transatlantic data privacy protections, and (3) the regulation of new technologies like artificial intelligence (AI) and blockchain. The aticle concludes with a list of recommendations for state and federal policymakers to consider in an effort to harden the IIoT along with the supply chains critical to the continued development of smart factories.*

---



* Chair, Indiana University-Bloomington Cybersecurity Program; Director, Ostrom Workshop Program on Cybersecurity and Internet Governance; Associate Professor, Indiana University Kelley School of Business. Special thanks to Keith Belton, Prof. Jenifer Sunrise Winter, Chris Peters, and Vishal Chawla for their helpful comments that were invaluable in developing this paper. This research was generously funded in part by a grant from the Indiana University O'Neil School for Public and Environmental Affairs (SPEA).

*Ubiquitous computing names the third wave in computing, just now beginning. First were mainframes, each shared by lots of people. Now we are in the personal computing era, person and machine staring uneasily at each other across the desktop. Next comes ubiquitous computing, or the age of calm technology, when technology recedes into the background of our lives.*

- Mark Weiser,[1] 1996

## INTRODUCTION

In 2015, for only the second time in history at that point, a cyberattack was confirmed to have caused physical damage.[2] The first such episode was Stuxnet.[3] This time, the target was not Iran's nuclear program, but a steel mill in Germany. Specifically, a blast furnace was compromised causing "'massive'—though unspecified—damage."[4] Attackers had gained access to the plant through the firm's business network, highlighting the insecurity that can stem from interconnected systems even when a firewall is in place.[5] There have been unconfirmed reports of similar incidents, such as one involving a petrochemical factory that was compromised by a coffee maker.[6] This issue is coming to the fore with the expansion of Internet-connected devices in the manufacturing sector. These

---

1. Personal website of Mark Weiser, UBIQUITOUS COMPUTING (Mar. 17, 1996, 8:00 PM), http://www.ubiq.com/hypertext/weiser/UbiHome.html [https://web.archive.org/web/20170214230140/http://www.ubiq.com/hypertext/weiser/UbiHome.html].

2. *See* Kim Zetter, *A Cyberattack Has Caused Confirmed Physical Damage for the Second Time Ever*, WIRED (Jan. 8, 2015, 5:30 AM), https://www.wired.com/2015/01/german-steel-mill-hack-destruction/ [https://perma.cc/4M49-2HTY] (describing a cyber attack on an unnamed German steel mill).

3. *See* Kim Zetter, *An Unprecedented Look at Stuxnet, the World's First Digital Weapon*, WIRED (Nov. 3, 2014, 6:30 AM), https://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/ [https://perma.cc/P5L3-LXCY] (describing the Stuxnet cyber attack on Iranian uranium enrichment centrifuges).

4. *See* Zetter, *supra* note 2.

5. *Id.*

6. *See* C10H15N1, *How the Coffee-Machine Took down a Factories Control Room*, REDDIT (July 22, 2017, 11:39:47 AM), https://www.reddit.com/r/talesfromtechsupport/comments/6ovy0h/how_the_coffeemachine_took_down_a_factories/ [https://perma.cc/86MP-NKRV] (describing a ransomware attack on wifi-enabled coffee machines, which spread to the factory control systems).

devices promise new efficiencies and innovations while also introducing new vulnerabilities.[7]

The Internet of Things (IoT) underscores the notion of a hyper-connected future.[8] As one example, McKinsey Consulting has estimated the economic impact of the Internet of Things, or what may be more accurately described as the "Network of Things,"[9] at $6.2 trillion by 2025.[10] The Industrial Internet of Things (IIoT), sometimes also called the "Factory of Things," or "Smart Factory Wave," involves the use of IoT technologies in manufacturing applications.[11] It holds the promise to revolutionize manufacturing, including in the fields of "factory health, digital thread, and smart products."[12] Already, a number of industrial control systems (ICS) manufacturers, such as Rockwell Automation, are offering a range of IIoT products from programmable controllers and industrial sensors to distributed

---

7. These include distributed denial of service attacks and botnets such as Mirai. *See generally,* Constantinos Kolias et al., *DDoS in the IoT: Mirai and Other Botnets*, 50 IEEE COMPUTER 80 (2017) (warning that the ubiquity of internet-connected devices provides a large and vulnerable platform that can be exploited by botnets to amplify cyberattacks).

8. *See generally* Scott J. Shackelford et al., *When Toasters Attack: A Polycentric Approach to Enhancing the "Security of Things,"* 2017 U. ILL L. REV. 415 (2017) (explaining the Internet of Things and associated challenges); *see also* Scott J. Shackelford & Scott Bradner, *Have You Updated Your Toaster? Transatlantic Approaches to Governing the Internet of Everything*, (Kelley Sch. of Bus., Res. Paper No. 18-60), https://papers.ssrn.com/sol3/papers.cfm ?abstract_id=3208018.

9. *See generally* Bernardo A. Huberman, *Ensuring Trust and Security in the Industrial IoT*, UBIQUITY, (Jan. 2016) https://ubiquity.acm.org/article.cfm?id=2822883 (describing the Internet of Things as a "network of small sensors that enables precise control and monitoring of complex processes over arbitrary distances.").

10. Chunka Mui, *Thinking Big About the Industrial Internet of Things*, FORBES (Mar. 4, 2016, 10:03 AM), https://www.forbes.com/sites/chunkamui /2016/03/04/thinking-big-about-industrial-iot/#7f1e54066220 [https://perma.cc/CHX5-QFFX].

11. *See* Richard D. Taylor, *The Next Stage of U.S. Communications Policy: The Emerging Embedded Infosphere*, 41 TELECOMM. POL'Y 1039, 1039 (2017) ("The United States needs to reimagine the basic principles of its telecommunications and information policy to fit an emerging society in which networking and intelligence are embedded into an increasing number of everyday things which constantly monitor and measure our lives. This emerging environment is an always-on, ubiquitous, integrated system comprised of the Internet of Things, Big Data, Artificial Intelligence/Intelligent Systems and the Intercloud, which act together as a single system, referred to here as the 'Embedded Infosphere' (EI).").

12. *See* Mui, *supra* note 10.

control systems.[13] However, while such products promote efficiency, they also increase the attack surface and with it the cyber risk that manufacturers must manage.[14]

Numerous outstanding cybersecurity and data privacy issues impact the realization of the myriad benefits promised by IIoT, including the use of personal data in factory settings.[15] Yet, to date, there has been a paucity of literature on the topic.[16] This

---

13. *See Product Offerings*, Rockwell Automation, https://www.rockwellautomation.com/en_NA/products/overview.page (last visited Dec. 20, 2019).

14. *See* Bob Tarzey, *The Ever-Growing IoT Attack Surface*, COMPUTER WEEKLY: QUOCIRCA INSIGHTS (July 6, 2017, 8:56 AM), https://www.computerweekly.com/blog/Quocirca-Insights/The-ever-growing-IoT-attack-surface [https://perma.cc/928Z-GP9S] (discussing IoT vulnerabilities).

15. *See, e.g.*, Randy Vogenberg et al., *Personalized Medicine*, 35 PHARMACY & THERAPEUTICS 624 (2010) (describing the application of this concept in the personalized medicine movement and discussing the fact that high-risk personal data is typically not covered under HIPAA).

16. *Cf.* Charles J. Barnes, *Smart Home Alone: The World's Gateway to More Efficient Use of Energy and Mayhem*, 5 LSU J. OF ENERGY L. & RESOURCES 365, 368 (2017) ("Industry leaders and Smart Grid regulators are pushing for greater interoperability within the Smart Grid. Although greater interoperability would be beneficial, if unchecked, this policy will lead to a kinetic cyber attack.") (footnote omitted); Nikole Davenport, *Smart Washers May Clean Your Clothes, but Hacks Can Clean out Your Privacy, and Underdeveloped Regulations Could Leave You Hanging on a Line*, 32 J. MARSHALL J. INFO. TECH. & PRIVACY L. 259, 262–63 (2016) ("The IoT is a broad concept used colloquially to encompass many or all of the interconnected devices in our future. But industry experts identify three subsets to the general IoT category which are the Industrial Internet (i.e. all interconnected products, sensors, controls, etc., used in industry and business), the Internet-of-everything (consumer objects and systems that combine people and data), and the Cyber physical systems (which are the systems that connect it all)."); Kevin DiGrazia, *Cyber Insurance, Data Security, and Blockchain in the Wake of the Equifax Breach*, 13 J. BUS. & TECH. L. 255, 262 (2018) ("Firms purchasing cyber insurance should understand what their current insurance policies will cover, and what duplicate coverage and peril gaps exist. With the surge in automation of the IoT and the Industrial Internet of Things ("[IIoT]"), hackers will increasingly be able to cause physical damage to machinery and other equipment."); Stacy-Ann Elvy, *Contracting in the Age of the Internet of Things: Article 2 of the UCC and Beyond*, 44 HOFSTRA L. REV. 839, 906 n.367 (2016) (noting that cyber attacks on the Industrial Internet of Things are increasing); Andrew G. Ferguson, *The Internet of Things and the Fourth Amendment of Effects*, 104 CALIF. L. REV. 805, 813 (2016) ("Experts predict that the worldwide scale of such 'smart,' interconnected objects will continue to grow, reaching more than fifty billion objects in 2020, and one trillion by 2025. As inexpensive, unobtrusive identifying technology combines with more sophisticated wireless networks, new possibilities will emerge to allow tracking of human and nonhuman activity. The result will be additional options for government surveillance that can reveal the patterns of everyday

article analyzes some of these gaps, focusing on: (1) critical infrastructure protection and cybersecurity due diligence, (2) trends in transatlantic data privacy protections relevant to manufacturers, and (3) the regulation of new technologies like AI and blockchain and their applicability to address IIoT security and privacy challenges. This article concludes with an analysis of options available to state and federal policymakers to help harden IIoT devices and supply chains against cyber attacks.

## I. CYBERSECURITY AND DATA PRIVACY IIOT HOT TOPICS

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.[17] But the idea has been around for longer, including as pervasive computing, "Ubiquitous Computing," and "Real-World Web."[18] Although these terms are not all analogous,[19] it is true that from these humble beginnings has come a global effort to make our technology, businesses, and

---

life.") (footnotes omitted); Dera J. Nevin & Marc Jenkins, *Information, Knowledge, and the Pursuit of Privacy*, 38 AM. J. TRIAL ADVOC. 485, 488–89 (2015) (arguing that "'Big Iron' companies like General Electric (GE) have become Big Data technology companies."); Dalmacio V. Posadas, Jr., *After the Gold Rush: The Boom of the Internet of Things, and the Busts of Data-Security and Privacy*, 28 FORDHAM INTELL. PROP. MEDIA & ENT. L. J. 69, 76 (2017) ("On a larger scale, the so-called Industrial IoT is streamlining industrial production across the world. However, what remains unclear is the depth and breadth of how these efficient objects will impact privacy.") (footnote omitted).

17. *See* Kevin Ashton, *That 'Internet of Things' Thing*, RFID J. (June 22, 2009), www.rfidjournal.com/articles/view?4986 [https://perma.cc/J638-8KN3] (describing one possible origin of the term).

18. *See* Jackie Fenn & Hung LeHong, *Hype Cycle for Emerging Technologies*, GARTNER (July 28, 2011), https://www.gartner.com/doc/1754719 /hype-cycle-emerging-technologies (explaining the Gartner "hype cycle." The "hype cycle" is a graphical model used by the I.T. firm Gartner to represent periods of excitement and disillusionment); *see* Detlef Zuehlke, *Smart-Factory: Towards a Factory-of-Things*, 34 ANN. REV. CONTROL 129, 129 (2010) (applying the concept of "ubiquitous computing"). *See also* Jennifer S. Winter, *Privacy, Algorithmic Discrimination, and the Internet of Things in* ENCYCLOPEDIA OF INFORMATION SCIENCE AND TECHNOLOGY 4951, 4951–52 (Medhi Khosrow-Pour ed., 2018) (applying the concepts of "ubiquitous computing" and "ambient intelligence").

19. *See* Winter, *supra* note 18 (discussing the difference between "ubiquitous computing" and "ambient intelligence.").

even our bodies, smart.[20] Wherever it came from, the term IoT today now enjoys widespread use in both technology and policy circles, as well as in popular culture.[21] It includes a constellation of devices and technologies with built-in wireless connectivity that "can be monitored, controlled[,] and linked"[22] together, as is represented in Figure 1.

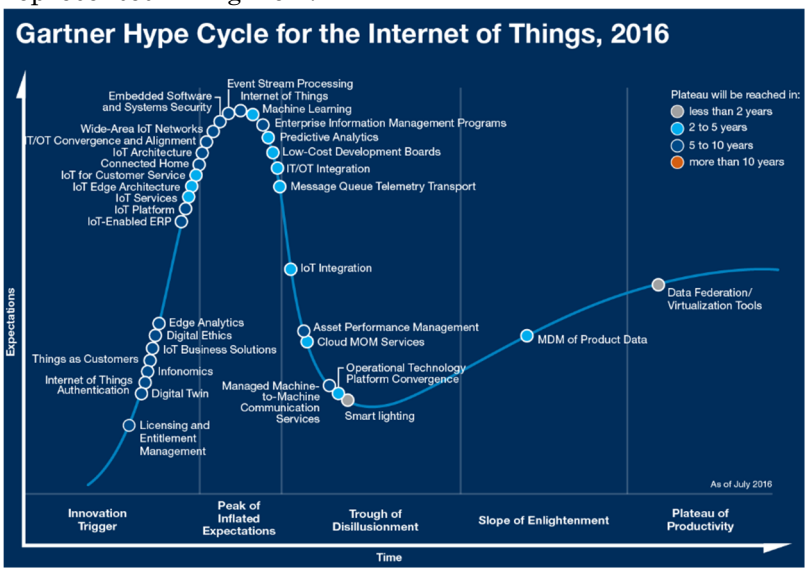


**Fig. 1 2016 Gartner IoT 'Hype Cycle'**[23]

The increasingly hyper-connected network of products and systems comprising IoT opens up new economic opportunities,

---

20. *See, e.g.*, Meghan Neal, *The Internet of Bodies is Coming, and You Could Get Hacked*, MOTHERBOARD (Mar. 13, 2014, 1:20 PM), https://motherboard.vice.com/en_us/article/gvyqgm/the-internet-of-bodies-is-coming-and-you-could-get-hacked [https://perma.cc/4YN5-GZEJ] (discussing the effort to augment bodies using implantable technology).

21. *See* Fenn & LeHong, *supra* note 18 (discussing contemporary use of the term "Internet of Things").

22. Bonnie Cha, *A Beginner's Guide to Understanding the Internet of Things*, RECODE (Jan. 15, 2015, 6:00 AM), https://www.recode.net/2015/1/15/11557782/a-beginners-guide-to-understanding-the-internet-of-things [https://perma.cc/6GE2-MC7G].

23. *Technologies Underpin the Hype Cycle for the Internet of Things, 2016*, GARTNER (Nov. 2, 2016), https://www.gartner.com/smarterwithgartner/7-technologies-underpin-the-hype-cycle-for-the-internet-of-things-2016/ (describing the Gartner "hype cycle" for IoT technology).

along with vulnerabilities.[24] Already, though, some of the excitement may be fading in the wake of well-publicized vulnerabilities, such as may be seen with smart lightbulbs already being in the "Trough of Disillusionment" in Figure 1. This section explores some of the security implications in the smart factory revolution, what has been called the "fourth revolution" in this space,[25] before moving on to analyzing the associated policy implications.

### A. SMART FACTORIES AND CRITICAL INFRASTRUCTURE PROTECTION

The U.S. Department of Homeland Security is tasked with defining and defending these vital industries, which it subdivides into sixteen sectors.[26] These sectors are not fixed; for example, elections were included under the public facilities

---

24. *See* Aaron Tilley, *How Hackers Could Use A Nest Thermostat As An Entry Point Into Your Home*, FORBES (Mar. 6, 2015, 6:00 AM), https://www.forbes.com/sites/aarontilley/2015/03/06/nest-thermostat-hack-home-network/#235d0d693986 [https://perma.cc/9VYV-ECT4]; Carl Franzen, *How to Find a Hack-Proof Baby Monitor*, OFFSPRING (Aug. 4, 2017, 6:30 PM), https://offspring.lifehacker.com/how-to-find-a-hack-proof-baby-monitor-1797534985 [https://perma.cc/T9ZQ-QE2X]; 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 Be the Next Hacker Target*, N.Y. TIMES (Nov. 3, 2016), https://www.nytimes.com/2016/11/03/technology/why-light-bulbs-may-be-the-next-hacker-target.html (providing examples of the threat hackers pose to smarter tech).

25. Hyoung Seok Kang et al., *Smart Manufacturing: Past Research, Present Findings, and Future Directions*, 3 INT'L J. PRECISION ENG'G & MFG.-GREEN TECH. 111, 118 (2016).

26. *See* Directive on Critical Infrastructure Security and Resilience, 2013 DAILY COMP. PRES. Doc. 92 (Fed. 12, 2013); *Supporting policy and Doctrine*, DHS, (last visited Dec. 20, 2019), https://www.dhs.gov/cisa/supporting-policy-and-doctrine [https://perma.cc/R22C-A3WN]; *Frequently Asked Questions*, (last visited Dec. 20, 2019) http://web.archive.org/web/20140117082728/http://ics-cert.us-cert.gov/Frequently-Asked-Questions (describing the U.S. Cyber Emergency Response Team, which is part of DHS, and identifying sixteen critical infrastructure sectors consistent with Homeland Security Presidential Directive 7 including: agriculture, banking and finance, chemical, commercial facilities, dams, defense industrial base, drinking water and water treatment systems, emergency systems, energy, government facilities, information technology, nuclear systems, public health and healthcare, telecommunications, and transportation systems).

sector in January 2017.[27] Smart factories fall under an array of critical infrastructure sectors, including the critical manufacturing sector itself (which comprises electrical equipment and appliances along with transportation) along with the communications, healthcare, and even the defense industrial base. As such, firms operating in this space should be aware of the possibility for substantial federal oversight, such as would have been required under the Cybersecurity Act of 2012.[28] Each of these sixteen sectors boasts an Information Sharing and Analysis Center (ISAC) to help spread cyber threat information, along with awareness as to best practices.[29] Efforts have also been made to break down silos between sectors, such as through Information Sharing and Analysis Organizations (ISAOs).[30] Such public-private bi-directional information sharing between the critical infrastructure sectors will be essential to defending the IIoT, including both information technology (IT) (e.g., business systems) and operations technology (OT) that cover those systems in the manufacturing environment.[31] The latter distinction is important since IT efforts typically prioritize their focus on confidentiality, integrity and then availability, while OT efforts place the highest priority on availability.

---

27. *See Statement by Secretary Jeh Johnson on the Designation of Election Infrastructure as a Critical Infrastructure Subsector*, DEP'T HOMELAND SEC. (Jan. 6, 2017), https://www.dhs.gov/news/2017/01/06/statement-secretary-johnson-designation-election-infrastructure-critical (designating "election infrastructure" as a critical infrastructure subsector).

28. *See* Scott J. Shackelford, *In Search of Cyber Peace: A Response to the Cybersecurity Act of 2012,* 64 STAN. L. REV. ONLINE 106 (Mar. 8, 2012), http://www.stanfordlawreview.org/online/cyber-peace (responding to the Cybersecurity Act of 2012).

29. *E.g.*, U.S. DEP'T OF HOMELAND SEC., CHEMICAL-SECTOR SPECIFIC PLAN (2015) ("The sector is currently pilot testing an Information Sharing and Analysis Center (ISAC) to facilitate the dissemination of cyber threat data between DHS, other government agencies, and the Chemical Sector.").

30. *See generally Information Sharing and Analysis Organizations (ISAOs)*, U.S. DEP'T HOMELAND SEC., https://www.dhs.gov/cisa/information-sharing-and-analysis-organizations-isaos [https://perma.cc/2YGZ-Z9HZ] (last visited Sept. 21, 2019) (providing a general overview of Information Sharing and Analysis Organizations).

31. *See* Amanda Ziadeh, *Homeland Security is Building Collective Defense Against Adversaries*, GOVT. CIO MEDIA (July 20, 2018, 3:57 PM), https://www.governmentciomedia.com/homeland-security-building-collective-defense-against-adversaries [https://perma.cc/ZNN5-FBTH] (advocating a joint effort between the government and the private sector to better combat cyber threats).

Compounding the challenge is that most existing OT systems do not have the capacity to add cybersecurity protections without negatively impacting production. This fact will be all the more important as threats to smart factories proliferate.

1. Threats from Foreign Nation-States and Economic Espionage Campaigns

In March 2018, the FBI and DHS jointly accused the Russian government of a "multi-stage intrusion campaign" targeting the U.S. power grid along with compromising the industrial control systems of several "small commercial facilities."[32] This episode is just one data point in a long history of cyber attacks on U.S. critical infrastructure with links to Russia.[33] The United States is far from alone. For example, Ukraine experienced waves of attacks including "the first-ever confirmed cyberattack against grid infrastructure."[34] Russia is not alone in its online aggression either, with the list of cyber powers growing to more than fifty nations, not to mention sophisticated criminal organizations, firms, and hacktivists.[35] Iran, for example, has reportedly readied a wave of cyber attacks

---

32. Taylor Hatmaker, *DHS and FBI Detail How Russia Is Hacking into U.S. Nuclear Facilities and Other Critical Infrastructure*, TECHCRUNCH (Mar. 15, 2018, 3:54 PM), https://techcrunch.com/2018/03/15/russia-energy-hack-dhs-fbi-us-cert/ [https://perma.cc/C9DC-HT74].

33. *See* OFFICE OF THE DIR. OF NAT'L INTELLIGENCE, JOINT DHS, ODNI, FBI STATEMENT ON RUSSIAN MALICIOUS CYBER ACTIVITY (Dec. 29, 2016) https://www.fbi.gov/news/pressrel/press-releases/joint-dhs-odni-fbi-statement-on-russian-malicious-cyber-activity (detailing Russian efforts to cyber attack the U.S. government and its citizens).

34. Jeff St. John, *The Real Cybersecurity Issues Behind the Overhyped 'Russia Hacks the Grid' Story*, GREENTECH (Jan. 4, 2017), https://www.greentechmedia.com/articles/read/the-real-cybersecurity-issues-behind-the-overhyped-russia-hacks-the-grid-st [https://perma.cc/6GGN-GFVQ].

35. *E.g.*, Keth Breene, *Who Are the Cyberwar Superpowers?*, WORLD ECON. F. (May 4, 2016), https://www.weforum.org/agenda/2016/05/who-are-the-cyberwar-superpowers/ [https://perma.cc/2NJY-38UG] (one list of potential nations designated as "cyber superpowers"); Elvis Plesky, *Top Hacking Groups Impacting Cybersecurity Today*, PLESK (July 3, 2018), https://www.plesk.com/blog/business-industry/top-hacking-groups-cybersecurity-today/ (listing various hacking groups and their histories); Shannon Vavra, *The World's Top Cyber Powers*, AXIOS (Aug. 13, 2017), https://www.axios.com/the-worlds-top-cyber-powers-1513304669-4fa53675-b7e6-4276-a2bf-4a84b4986fe9.html [https://perma.cc/DC7W-ZVKX] (listing the world's top cyberpowers and the types of attacks they are capable of launching).

against critical infrastructure in response to the United States' withdrawal from the Iran nuclear agreement.[36]

Yet the threat of cyber conflict is also only one facet in the multi-faceted cyber risk facing smart factories. Another facet is the continued prevalence of trade secrets theft, even after the U.S.-China 2015 Cybersecurity Code of Conduct, which was designed to safeguard commercial intellectual property and was prompted in part by hackers targeting U.S. Steel.[37] The rise of IIoT generally, and smart factories in particular, has expanded the threat surface against which manufacturers will have to protect their systems and property, necessitating advances in cybersecurity due diligence. In one demonstration, for example, a single compromised wireless webcam was able to "jam all wireless communication and thereby stop production" at a factory.[38] Other threats are numerous and can emanate from an array of actors such as criminal organizations, terrorist groups, insider threats, and intellectual property thieves.[39]

### 2. Meaning of "Cybersecurity Due Diligence" for Smart Factories

"Due diligence" has a multitude of meanings depending on the context, nation, and sector involved.[40] In the transactional

---

36. *See* Courtney Kube et al., *Iran has Laid Groundwork for Extensive Cyberattacks on U.S., Say Officials*, NBC NEWS (July 20, 2018, 10:50 AM), https://www.nbcnews.com/news/us-news/iran-has-laid-groundwork-extensive-cyberattacks-u-s-say-officials-n893081 [https://perma.cc/W8VR-W49Q] ("Iranian hackers have laid the groundwork to carry out extensive cyberattacks on U.S. and European infrastructure and on private companies . . . .").

37. *See* Gary Brown & Christopher D. Yung, *Evaluating the US-China Cybersecurity Agreement, Part I: The US Approach to Cyberspace*, DIPLOMAT (Jan. 19, 2017), https://thediplomat.com/2017/01/evaluating-the-us-china-cybersecurity-agreement-part-1-the-us-approach-to-cyberspace/; Colin Hanna, *China Stonewalls U. S. Steel's Cybertheft Lawsuit*, INVESTOR'S BUSINESS DAILY (Mar. 27, 2017), https://www.investors.com/politics/commentary/china-stonewalls-u-s-steels-cyber-theft-lawsuit/ [https://perma.cc/2EFJ-3WRR].

38. Zuehlke, *supra* note 18, at 136.

39. *See generally* 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, 12–13 (2015) (detailing potential cyber threats to trade secrets).

40. *See, e.g.,* Scott J. Shackelford et al., *Unpacking the International Law on Cybersecurity Due Diligence: Lessons from the Public and Private Sectors*. 17 Chi. J. Int'l L. 1, 7–20 (2016) (discussing different standards of cybersecurity due diligence in caselaw).

context, cybersecurity due diligence has been defined as "the review of the governance, processes, and controls that are used to secure information assets."[41] This broad understanding builds from the corporate, national, and international obligations of both state and non-state actors to help identify and instill cybersecurity best practices across a range of actors.[42] Such a broad, multidisciplinary understanding of this concept is vital in the IoT context in particular, given the extent to which networks and systems interact. Here, cybersecurity due diligence is centered on identifying and spreading risk management best practices between State and non-State actors, so as to promote security in smart manufacturing. One illustration is the Governance, Risk, and Compliance (GRC) Framework, which considers the "capabilities that integrate the governance, management and assurance of performance, risk, and compliance activities" across an organization.[43] The question becomes how manufacturers can fulfill GRC responsibilities, which include not just protecting technical infrastructure, but also safeguarding trade secrets and sensitive personal data that may be subject to big data analytics and deep learning. The next section discusses this topic.[44]

---

41. Tim Ryan & Leonard Navarro, *Cyber Due Diligence: Pre-Transaction Assessments Can Uncover Costly Risks,* KROLL (Jan. 28, 2015), https://www.kroll.com/en/insights/publications/cyber/cyber-due-diligence-pre-transaction-assessments [https://perma.cc/AW3X-Z43H].

42. *See generally* 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/ (discussing the concept of "cyber peace" and the role that state and non-state actors play in maintaining cyber peace).

43. *What is GRC?*, OCEG, https://www.oceg.org/about/what-is-grc/ [https://perma.cc/X47X-289D] (last visited Nov. 27, 2019).

44. In general, data privacy policies are needed to cover proprietary manufacturing data generated by the IIoT. Such data may range from the code that runs machines to the output of sensors that measure recipe amounts and composition. There are a number of situations where such data may be captured and aggregated by supply chain partners, equipment manufacturers, and others. The lack of a clear delineation of ownership is an impediment for companies to connect their IIoT systems to each other, reducing the benefits of digital manufacturing.

### 3. Federal Cybersecurity Frameworks and Standards Impacting Smart Factories

Two of the main efforts aimed at defining cybersecurity due diligence that are most relevant to the smart factory context are the National Institute of Standards and Technology Cybersecurity Framework (NIST CSF) and the Federal Trade Commission's (FTC) guidance.[45] The NIST CSF was born from President Obama's efforts to empower NIST to partner with industry and develop a framework comprised of private-sector cybersecurity best practices that would help inform an array of organizations in their cybersecurity decision-making processes, but particularly those operating critical infrastructure.[46] The result was the first NIST CSF, in 2014. While critics have complained about the framework's reactive stance,[47] it nevertheless is helping to define cybersecurity due diligence in the United States.[48] The NIST CSF takes manufacturing concerns into account; indeed, NIST deserves credit for focusing its efforts on improving cybersecurity due diligence in factories, as seen in its published Cybersecurity Framework Manufacturing Profile that is "a roadmap for reducing

---

45. *See* NAT'L INST. OF STANDARDS AND TECH., IMPROVING CRITICAL INFRASTRUCTURE CYBERSECURITY EXEC. ORDER 13636: PRELIMINARY CYBERSECURITY FRAMEWORK 1 (2013).

46. *See NIST Marks* Fifth *Anniversary of Popular Cybersecurity Framework*, NIST (Feb. 12, 2019), https://www.nist.gov/news-events/news/2019/02/nist-marks-fifth-anniversary-popular-cybersecurity-framework [https://perma.cc/PQ5R-2HLH].

47. *See, e.g.*, 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 [https://perma.cc/W9C4-7WL2] (describing a critique of the NIST CSF as being backward-looking, rather than forward-looking).

48. *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) (analyzing the impact of the Cybersecurity Framework on domestic industry and the international landscape); Scott J. Shackelford, Scott Russell, & Andreas Kuehn, *Unpacking the International Law on Cybersecurity Due Diligence: Lessons from the Public and Private Sectors*, 17 CHI. J. INT'L L. 1, 1 (2016) (arguing for a "proactive regime" in the public and private sector that draws off the NIST framework).

cybersecurity risk for manufacturers."[49] Rather than replace security policies already in effect, NIST intends these "voluntary, risk-based" efforts to enhance existing commitments and support organizations in their efforts to "identify, implement, and improve cybersecurity practices, and create[] a common language for internal and external communication of cybersecurity issues."[50] The original NIST CSF was voluntary,[51] but advocates have increasingly made the case that if an organization's "cybersecurity practices were ever questioned during litigation or a regulatory investigation, the 'standard' for 'due diligence' was now the NIST [CSF]."[52] While it was originally published in 2014, NIST has remained engaged in this space,[53] as seen in the development of the 2018 NIST Privacy Framework,[54] and the 2016 NIST CSF for small businesses,[55] all of which are important data points for boosting cybersecurity and privacy due diligence in the smart manufacturing context.

The NIST CSF not only has the potential to gradually shape a standard of care for domestic manufacturing, but also could help to harmonize global cybersecurity best practices for given active NIST collaborations with more than twenty nations

---

49. KEITH A. STOUFFER ET AL., NAT'L INST. OF STANDARDS AND TECH., CYBERSECURITY FRAMEWORK MANUFACTURING PROFILE, NISTIR 8183 (2017), https://doi.org/10.6028/NIST.IR.8183.

50. *Why You Should Adopt the NIST Framework* 1, PWC (May 2014), https://www.pwc.com/us/en/increasing-it-effectiveness/publications/assets/adopt-the-nist.pdf [https://perma.cc/7RFW-4MEM].

51. NAT'L INST. OF STANDARDS AND TECH., FRAMEWORK FOR IMPROVING CRITICAL INFRASTRUCTURE CYBERSECURITY (2015), *available at* https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf.

52. John Verry, *Why the NIST Cybersecurity Framework Isn't Really Voluntary*, PIVOT POINT SECURITY: BLOG (Feb. 25, 2014), https://www.pivotpointsecurity.com/blog/nist-cybersecurity-framework [https://perma.cc/DW4R-EKBT] (discussing guidance given to Municipal Utility Districts).

53. *See*, NAT'L INST. OF STANDARDS AND TECH, NIST RELEASES VERSION 1.1 OF ITS POPULAR CYBERSECURITY FRAMEWORK (Apr. 16, 2018), https://www.nist.gov/news-events/news/2018/04/nist-releases-version-11-its-popular-cybersecurity-framework [https://perma.cc/77XX-FGG9] (announcing the release of updated standards based on user feedback).

54. Developing a Privacy Framework, 83 Fed. Reg. 56824 (Nov. 14, 2018) (requesting comment on proposed updates to the privacy framework).

55. NAT'L INST. OF STANDARDS AND TECH., SMALL BUSINESS INFORMATION SECURITY: THE FUNDAMENTALS (2016), https://nvlpubs.nist.gov/nistpubs/ir/2016/NIST.IR.7621r1.pdf.

including the United Kingdom, Japan, South Korea, Israel, and Germany.[56] Such a global push is particularly important in the manufacturing sector given the extent to which supply chains straddle jurisdictions, and even continents.[57] Progress toward further defining baseline cybersecurity due diligence in the manufacturing context 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."[58] The new version boasts significant improvements, including modernized policies regarding authentication, supply chain cybersecurity, and vulnerability disclosure.[59] Yet, the NIST CSF is still best considered a cybersecurity floor rather than a ceiling. It does not, for example, focus on IoT issues in particular, which is an area that many would like NIST to address in more detail as is discussed further below.

Similar to NIST, commentators have made the case that the FTC suggests "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."[60] In particular, the FTC suggests keeping software updated, encrypting sensitive data, using multi-factor authentication, and having an updated incident response plan.[61]

---

56. The FTC's enforcement powers may already be facilitating the development of these best practices. *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/.

57. *See, e.g.*, Maria Korolov, *What Is a Supply Chain Attack? Why You Should Be Wary of Third-Party Providers*, CSO (Apr. 4, 2018, 8:15 AM), https://www.csoonline.com/article/3191947/data-breach/what-is-a-supply-chain-attack-why-you-should-be-wary-of-third-party-providers.html [https://perma.cc/DP24-QV5Q]; Warwick Ashford, *Most Businesses Vulnerable to Supply Chain Cyber Attacks*, COMPUT. WEEKLY (Apr. 30, 2019, 11:30 AM), https://www.computerweekly.com/news/252462476/Most-businesses-vulnerable-to-supply-chain-cyber-attacks [https://perma.cc/MH2P-FSPA].

58. NAT'L INST. OF STANDARDS & TECH., *supra* note 53.

59. *Id*.

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

61. *See Cybersecurity Basics*, FED. TRADE COMM'N, https://www.ftc.gov/tips

The FTC is able to give such suggestions binding legal force thanks to Section Five of the Federal Trade Commission Act, which established the FTC and empowers it to police "unfair or deceptive acts or practices."[62] The FTC has wielded this authority to penalize firms for lax privacy and cybersecurity standards.[63] The United States Court of Appeals for the Third Circuit upheld the FTC's power in this regard in 2015 in *FTC v. Wyndham Worldwide*.[64] However, a 2018 case, *LabMD Inc. v. Federal Trade Commission*, underscored a potential growing circuit split involving the FTC, which may require it to be more specific in the cybersecurity requirements it places on businesses.[65] This could include requiring more firms to take measures that so far the FTC has only encouraged on a voluntary basis, including:

> * [B]uild security into devices at the outset, rather than as an after-thought in the design process;
>
> * [T]rain employees about the importance of security, and ensure that security is managed at an appropriate level in the organization;
>
> * [E]nsure that when outside service providers are hired, that those providers are capable of maintaining reasonable security, and provide reasonable oversight of the providers;
>
> * [W]hen a security risk is identified, consider a "defense-in-depth" strategy whereby multiple layers of security may be used to defend against a particular risk;

---

-advice/business-center/small-businesses/cybersecurity/basics (last visited Nov. 10, 2019) (encouraging small business owners to adopt the listed practices).

62. 15 U.S.C. § 45; *See also A Brief Overview of the Federal Trade Commission's Investigative and Law Enforcement Authority*, FED. TRADE COMM'N (2008), https://www.ftc.gov/about-ftc/what-we-do/enforcement -authority (describing the ability of the FTC to investigate and enforce as necessary).

63. *See Privacy & Data Security Update: 2018,* FED. TRADE COMM'N (2018), https://www.ftc.gov/system/ files/documents/reports/privacy-data-security -update-2018/2018-privacy-data-security-report-508.pdf (describing recent enforcement actions brought by the FTC).

64. FTC v. Wyndham Worldwide Corp., 799 F.3d 236, 248–249 (3rd Cir. 2015). *See also* W. Reece Hirsch & Rahul Kapoor, *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.

65. LabMD, Inc. v. FTC, 894 F.3d 1221, 1237 (11th Cir. 2018) (finding an FTC cease and desist order unenforceable for failing to enjoin "a specific act or practice" and requiring the business in question improve its "data security program to meet an indeterminable standard of reasonableness.").

> * [C]onsider measures to keep unauthorized users from accessing a consumer's device, data, or personal information stored on the network;
> * [M]onitor connected devices throughout their expected life cycle, and where feasible, provide security patches to cover known risks.[66]

However, due to complex supply chains and a global customer base, U.S. federal IoT regulations are by no means the only ones IIoT proponents must consider. The next section considers the impact of the State of California's recent efforts before moving on to discuss the European Union's regulatory efforts at cybersecurity and data privacy in the smart manufacturing sector.

4. State-Level IIoT Policy: California Case Study

California's 2018 Consumer Privacy Act is helping set a new standard for U.S. Privacy protections, following in the footsteps of its groundbreaking 2002 privacy law that ushered in the first data breach notification standards.[67] This latter idea has since been copied by the other 49 states[68] and the European Union[69] as is discussed further in the next subsection. Although the 2018 Privacy Act[70] does not go quite as far as the European Union's new General Data Protection Regulation (GDPR)[71] discussed below, it does include provisions that allow consumers to sue over data breaches, and obtain information about how their data is being gathered and used by companies to make more informed decisions.[72] Although there remains debate about the scope and

---

66. *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.

67. Cal. Civ. Code §§ 1798.29, 1798.82 (Deering 2002).

68. Computer Crime Statutes, NAT'L CONF. OF ST. LEGISLATURES, http://www.ncsl.org/research/telecommunications-and-information-technology/computer-hacking-and-unauthorized-access-laws.aspx#Hacking (last updated June 14, 2018).

69. *See* Council Regulation 2016/679, art. 85, 2016 O.J. (L 119) 1.

70. California Consumer Privacy Act 2018, Cal. Civ. Code §§1798.100–.199 (Deering 2019).

71. Council Regulation 2016/679, art. 1, 2016 O.J. (L 119) 1.

72. *See* Ben Adler, *California Passes Strict Internet Privacy Law with Implications for the Country*, NPR (June 29, 2018) https://www.npr.org/2018/06/29/624336039/california-passes-strict-internet-privacy-law-with-implications-for-the-country [https://perma.cc/U3RG-STY9] (describing the privacy implications of the law).

effectiveness of this intervention,[73] the law may well help shape the cybersecurity practices of the manufacturing base in California along with their business partners, such as by requiring added efforts to protect the privacy rights of consumers and suppliers.[74]

This law builds on California's existing IoT policies. One of these relevant efforts dates back to 2016, when 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."[75] This definition is still narrower than that applicable in the EU under the GDPR—where even a person's IP address is considered Personally Identifiable Information (PII)—but it should be considered a step in that direction.[76] In addition, California law requires "companies that share such information to not only take extra security precautions themselves when managing the information, but to ensure that any entities they share information with also abide by strict security measures."[77] Indeed, in practical effect, this regulation requires covered firms to include "contractual provisions mandating implementation of reasonable security measures."[78] This requirement could have an even greater impact on cybersecurity due diligence overall given the size of California's

---

73. *See* Jeff Kosseff, *Ten Reasons Why California's New Data Protection Law is Unworkable, Burdensome, and Possibly Unconstitutional (Guest Blog Post)*, TECH. & MARKETING L. BLOG (July 9, 2018), https://blog.ericgoldman.org/archives/2018/07/ten-reasons-why-californias-new-data-protection-law-is-unworkable-burdensome-and-possibly-unconstitutional-guest-blog-post.htm [https://perma.cc/959C-RN24] (summarizing regulatory and constitutional issues concerning with the new California data protection law).

74. *See, e.g.*, California Consumer Privacy Act 2018, Cal. Civ. Code § 1798.100(a) (Deering 2019) ("A consumer shall have the right to request that a business that collects a consumer's personal information disclose to that consumer the categories and specific pieces of personal information the business has collected.").

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

76. *See What is Personal Data?*, EU GDPR COMPLIANT, https://eugdprcompliant.com/personal-data/ (last visited Jan. 10, 2019).

77. Cook, *supra* note 75.

78. *Id*.

economy—which is bigger than the UK's as of 2018.[79] California's regulatory regime could further promote the global acceptance of both the NIST CSF and the FTC cybersecurity efforts discussed above.

### B. TRANSATLANTIC APPROACHES TO DATA PRIVACY IN THE INDUSTRIAL IOT CONTEXT

As discussed above, the cybersecurity and data privacy regime within the United States is sector-specific. In contrast, the European Union has taken a distinct and far more regulatory and comprehensive approach.[80] Examples include the 2018 passage of the Network Information Security (NIS) Directive, and the enactment of the GDPR, both of which are explored in this section. The EU approach is not without its critics, such as those who are concerned about over-centralization,[81] but it is equally true that these efforts have made the EU a global leader in information governance best practices.[82] Moreover, transatlantic approaches to how organizations should manage their cyber risk are converging around the language of risk management. The EU's Network

---

79. *See* Lisa M. Segarra, *California's Economy Is Now Bigger Than All of the U.K.*, FORTUNE (May 5, 2018), http://fortune.com/2018/05/05/california-fifth-biggest-economy-passes-united-kingdom/.

80. *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) (discussing the differences between EU and US stances on internet governance through an analysis of the decision in Schrems v. Data Protection Commissioner, ECJ Judgment in Case C-362/14 (2015) (Eur.)).

81. *Response to EU Cybersecurity Strategy and Proposed Directive on Network and Information Security (NIS)*, DIGITALEUROPE (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.").

82. No other nations, for example, have taken the U.S. approach to data privacy protection. *See* Mark Scott & Laurens Cerulus, *Europe's New Data Protection Rules Export Privacy Standards Worldwide*, POLITICO (Jan. 31, 2018 12:00 PM), https://www.politico.eu/article/europe-data-protection-privacy-standards-gdpr-general-protection-data-regulation/ [https://perma.cc/85FR-NP25] (describing the European Union's data privacy standards as "de facto global standards for most countries except for a few holdouts like China, Russia and the United States.").

Information Security Public-Private Platform (NIS Platform) takes a risk management approach, and specifically adopts the NIST CSF core—identify, protect, detect, respond, recover—as the industry-standard EU approach for cybersecurity policy.[83] As such, this aspect of EU data governance underscores the extent to which the transatlantic approach to both cybersecurity and privacy is increasingly using both the language and tools of risk management introduced above.

As with cybersecurity and information privacy generally, the EU has long been engaged with IoT issues.[84] For example, the EU founded the Alliance for Internet of Things Innovation.[85] The European Commission has also engaged internationally, welcoming delegations from around the world to discuss IoT governance,[86] reinforcing the EU's place as a leader for cybersecurity and privacy governance. Finally, in late 2015 the European Commission launched Horizon 2020, which included goals for smart cities and IoT deployment,[87] policies that are further reinforced by the EU's push to create a Digital Single Market in Europe to support the estimated eleven-trillion-dollar

---

83. *Compare* NIS Platform (WG-1) Final Draft 220515, Network and Information Security Risk Management Organisational Structures and Requirements, 13–15 (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) (considering the "Identify, Protect, Detect, Respond, Recover" model its discussion of methods "to ensure effective risk management"), *with* NAT'L INST. OF STANDARDS AND TECH *supra* note 53, at 6–7 (outlining the "Framework Core Functions:" identify, protect, detect, respond, and recover). For more on this topic, *see* Shackelford *supra* note 56.

84. *See Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee, and the Committee of the Regions*, at 2–3, COM (2009) 278 final (June 18, 2009) (explaining that adoption of IoT depends on privacy protections, as these protections are a prerequisite for social acceptance).

85. *The Alliance for Internet of Things Innovation (AIOTI)*, EUROPEAN COMM'N (Aug. 2, 2018), https://ec.europa.eu/digital-single-market/en/alliance -internet-things-innovation-aioti.

86. *Cf. Meeting with Brazilian Delegation, 28 May*, AIOTI NEWS, https://aioti.eu/meeting-with-brasilian-delegation-28-may/ ("Brazilian delegation presented their IoT strategy and was interested in smart farming and health. This exchange will be continued by AIOTI sending note with proposals of concrete cooperation areas.").

87. *See* European Commission Decision on Horizon 2020, O.J. C(2015) 6776 of 13 October 2015 (identifying five pilot areas including smart living as part of a broader movement toward IoT development).

economic impact of IoT applications by 2025.[88] The latter is only one component in the "Digitising European Industry" initiative, which includes three pillars for IoT policy across the EU, including: "a thriving IoT ecosystem; a human-centered IoT approach; [and] a single market for IoT."[89] The proposed 2017 "European Data Economy" initiative would strengthen the move toward a single market for IoT across Europe.[90] In short, the EU is balancing between an embrace of the IoT and the economic opportunities it affords,[91] while also taking proactive steps to address its downsides, including by clarifying its own liability regimes.[92] These goals demonstrate how the EU is planning to secure the full gamut of IoT devices, including those in the manufacturing sector.

1. Impact of GDPR

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) introduced above. 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,[93] an important goal of the GDPR is to tear down, to the

---

88. *See, e.g.*, *The Internet of Things*, EUROPEAN COMM'N, https://ec.europa.eu/digital-single-market/en/internet-of-things (last updated Sept. 19, 2019) (discussing the single digital market); *The 2019 State of IoT Report*, PARTICLE, https://www.particle.io/solutions/2019-state-of-iot-report/ (last visited Nov. 11, 2019) (proposing that "IoT will have a total potential economic impact of up to $11.1 trillion a year by 2025.").

89. *Id*.

90. *Id*.

91. *See, e.g.*, *Research & Innovation in Internet of Things*, EUROPEAN COMMI'N (Aug. 22, 2019), https://ec.europa.eu/digital-single-market/en/research-innovation-iot (identifying five IoT "large scale pilots" covering relevant IoT areas).

92. *See Liability for Emerging Digital Technologies* 2 (Commission Staff Working Document, Apr. 25, 2018), https://ec.europa.eu/digital-single-market/en/news/european-commission-staff-working-document-liability-emerging-digital-technologies [https://perma.cc/RAT2-FU8U] ("[A] reflection on future needs and developments is needed, not only from the perspective of the victim i.e. in order to ensure equitable remedies, compensation and allocation of responsibility, but also from the perspective of the innovators and companies operating in the EU as legal certainty is a key element for good business development.").

93. *See, e.g.,* Scott & Laurens, *supra* note 82.

extent feasible, remaining regulatory walls between the EU Member States and move toward a single EU market.[94]

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 seventy-two hours of a firm becoming aware of the incident and then conducting a post-mortem to ensure that a similar scenario will not recur.[95] 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 is "no level zero defined for the security and privacy of connected and smart devices. . . . [or] . . . legal guidelines for trust of IoT devices and services."[96] Further, European-level regulation is slow, and a blunt instrument—GDPR, as one example, took more than four years to be adopted after having been proposed in 2012.[97]

Microsoft has argued that for manufacturing firms at least, "[t]he message is clear: manufacturers, even outside Europe, need to consider their exposure under the GDPR and plan accordingly."[98] More specifically, according to Olivier Van Hoof of the data management firm Collibria:

---

94. *See Digital Single Market: Bringing Down Barriers to Unlock Online Opportunities*, EUROPEAN COMMISSION, https://ec.europa.eu/commission/priorities/digital-single-market_en (last visited Aug. 24, 2019) (explaining how regulatory barriers must be removed in favor of a single market in order to benefit from digital technologies most efficiently).

95. *See* Rita Heimes, *Top 10 Operational Impacts of the GDPR: Part 1 – Data Security and Breach Notification*, INT'L ASSOC. PRIVACY PROF. (Jan. 6, 2016), https://iapp.org/news/a/top-10-operational-impacts-of-the-gdpr-part-1-data-security-and-breach-notification/ [https://perma.cc/7E2B-TBDN] (discussing how the GDPR raised standards of breach notifications).

96. *Infineon – NXP – STMicroelectronics-ENISA Common Positon on Cybersecurity* 1 (Dec. 2016) https://www.enisa.europa.eu/publications/enisa-position-papers-and-opinions/infineon-nxp-st-enisa-position-on-cybersecurity.

97. *See, e.g.*, Scott Gordon, *Will We Get a GDPR for the IOT?*, SC MAGAZINE (Apr. 26, 2018), https://www.scmagazineuk.com/will-we-get-a-gdpr-for-the-iot/article/758037/ (arguing that the industry should establish standards for IoT security because regulation will not be enacted fast enough to address rapidly-developing privacy issues).

98. Çağlayan Arkan, *Achieving GDPR Compliance in Manufacturing*, MICROSOFT (Dec. 15, 2017), https://cloudblogs.microsoft.com/industry-blog/industry/manufacturing/achieving-gdpr-compliance-in-manufacturing/ [https://perma.cc/W2XR-JKCU].

> "[GDPR] has particular relevance for the manufacturing industry, which is using AI and RFID [Radio Frequency Identification] to collect, use and integrate personal information into product manufacturing. Through IoT and their quest to make better connections with end users, manufacturers are collecting more information about consumers. And we've seen a number of studies indicating the manufacturing industry lags behind in cybersecurity. Therefore, specific safeguards should be established for these newer forms of electronic communications and sharing of personal data. And it shouldn't be taken lightly. Regulators will issue significant fines for GDPR non-compliance, up to 2-4% of global revenue for non-compliance. The deadline for compliance . . . [was] May 25, 2018."[99]

As such, as with the California laws discussed above, the global impact of GDPR on the manufacturing sector should not be underestimated, and neither should the NIS Directive.

2. Applicability of NIS Directive to Smart Factories

Directives such as NIS 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.[100] However, these directives risk sacrificing consistency across the EU, along with the timeliness that is so critical in rapidly-evolving areas such as IoT innovation.[101] This author has argued 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."[102] However, EU directives are unlike regulations in that they are more nation-specific. Some variation is already apparent. For

---

99. Craig Guillot, *What American Manufacturers Need to Know About New Data Protection Laws in Europe*, CHIEF EXEC. GRP. (May 31, 2017), https://chiefexecutive.net/american-manufacturers-need-know-new-data-protection-laws-europe/.

100. *See* 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. (describing new EU rules that apply to all "critical operators" in "energy, transport, health and banking.").

101. *See generally Applying EU Law*, Eur. Comm'n https://ec.europa.eu/info/law/law-making-process/applying-eu-law_en [https://perma.cc/98ES-XJQE] (last visited Jan. 10, 2019) (providing additional information on the distinction between directives and regulations in the EU context).

102. Shackelford, Russell, & Haut, *supra* note 56, at 222–23.

example, the French government is considering mandating liability for security lapses on the part of IoT manufacturers.[103] This is similar to the different approaches being taken by U.S. states when it comes to IoT security.

### C. APPLICABILITY OF BLOCKCHAIN TECHNOLOGY TO MANAGING SUPPLY CHAIN RISKS

It is well-known that hackers can exploit vulnerabilities in software such as by sending users virus-infected emails or compromised links.[104] It is less well-known that attackers can also meddle with computers by altering the hardware on which the software runs.[105] These weaknesses are physical, and one might think they are therefore easier to identify than spotting a bug in millions of lines of code. In fact, they can be just as difficult to locate, if not more so.[106] As aforementioned, the supply chains for many firms are complex and frequently span dozens of jurisdictions and potentially hundreds of suppliers. Apple's iPhone, for example, relies on hundreds of suppliers from around the world.[107] Each of these steps in the manufacturing process introduces opportunities for security problems to arise. Recent research suggests that hackers could use smartphone apps to damage manufacturing equipment, or even destroy entire factories.[108] While no such large-scale disaster has yet taken place, even sophisticated retailers like Amazon have been

---

103. *See* Gordon, *supra* note 97.

104. *See, e.g.*, Arun Vishwanath, *'Spearphishing' Roiled the Presidential Campaign – Here's How to Protect Yourself*, CONVERSATION (Nov. 8, 2016), https://theconversation.com/spearphishing-roiled-the-presidential-campaign-heres-how-to-protect-yourself-68274.

105. *See* Andy Greenberg, *This 'Demonically Clever' Backdoor Hides in a Tiny Slice of a Computer Chip*, WIRED (June 1, 2016), https://www.wired.com/2016/06/demonically-clever-backdoor-hides-inside-computer-chip/.

106. Kaiyuan Yang et al., *A2: Analog Malicious Hardware*. IEEE, 23–25 May 2016 at 18. https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=7546493.

107. *See, e.g.*, Ian Baker, *The Global Supply Chain Behind the iPhone 6*, BETANEWS (2014), https://betanews.com/2014/09/23/the-global-supply-chain-behind-the-iphone-6/.

108. *See* Martin Giles, *Hackers Could Blow Up Factories Using Smartphone Apps*, MIT TECH. REV. (Jan. 11, 2018), https://www.technologyreview.com/s/609946/hackers-could-blow-up-factories-using-smartphone-apps/ (describing vulnerabilities in the control systems of some automated factories).

fooled by counterfeit facsimiles of real products.[109] Some supply chain threats are more malicious. In 2012, Microsoft warned customers that malware was being loaded onto computers made in China "after they were shipped to a distributor."[110] Even innocent motives may underlie serious problems. In 2015, Lenovo installed advertising software on its computers, which had the effect of dangerously weakening system security.[111] It is also distinctly possible that government actors could compromise the supply chain for the purposes of espionage.[112] These issues are particularly problematic in the IIoT context as more technology is deployed in factories, expanding economic opportunities as well as the attack surface that manufacturers must defend.

One new way to help secure such complex supply chains involves blockchain technology. The blockchain is a decentralized database that can be stored and maintained across

---

109. *See* Ari Levy, *Amazon's Chinese Counterfeit Problem Is Getting Worse*, CNBC (July 8, 2016), https://www.cnbc.com/2016/07/08/amazons-chinese-counterfeit-problem-is-getting-worse.html (explaining that Amazon is not able to combat the influx of Chinese counterfeit products. If Amazon is not able to spot counterfeits, an industrial producer could be similarly fooled).

110. *See Malware Being Installed on Computers in Supply Chain, Warns Microsoft*, GUARDIAN (Sept. 14, 2012), https://www.theguardian.com/technology/2012/sep/14/malware-installed-computers-factories-microsoft (describing an incident in which malware was loaded onto hardware while still in the distributor's supply chain).

111. *See* Elizabeth Weise, *FTC Settles with Lenovo Over a Built-In Snooping Software, $3.5 Million Fine*, USA TODAY (Sept. 5, 2017), https://www.usatoday.com/story/tech/2017/09/05/ftc-settles-lenovo-over-built-snooping-software-scanned-users-computers/632775001/ [https://perma.cc/FD24-UD9K] (Lenovo settled with the FTC regarding claims its laptops included preinstalled software that could potentially be exploited to obtain users' sensitive personal information); Joshua A.T. Fairfield, *The 'Internet of Things' Is Sending Us Back to the Middle Ages*, CONVERSATION (Sept. 5, 2017), https://theconversation.com/the-internet-of-things-is-sending-us-back-to-the-middle-ages-81435 (Lenovo's software "hijacked web browsers' traffic without the user's knowledge – including web communications users thought were securely encrypted, like connections to banks and online stores for financial transactions.").

112. *See, e.g.*, T.C. Sottek, *NSA Reportedly Intercepting Laptops Purchased Online to Install Spy Malware*, VERGE (Dec. 29, 2013), https://www.theverge.com/2013/12/29/5253226/nsa-cia-fbi-laptop-usb-plant-spy (claiming the NSA is able to intercept computers and use advanced hacking tools to plant spy software without the owner's permission or knowledge).

myriad systems.[113] Blockchain technology, for example, could be used to track and verify the inputs into complicated supply chains like Apple's.[114] Futurist Bernard Marr has argued that, "[u]ltimately, blockchain can increase the efficiency and transparency of supply chains and positively impact everything from warehousing to delivery to payment. Chain of command is essential for many things, and blockchain has the chain of command built in."[115] The Australian car manufacturer Tomcar, for example, pays its suppliers using Bitcoin.[116] Major multinational firms such as Unilever, Nestle, Tyson, Dole, and Walmart already use blockchain applications to keep track of food sources.[117] However, no blockchain is immune to hacking.[118] Policymakers around the world are taking a hard look at appropriate blockchain regulations, with divergent approaches being tried from Albany to Brussels.[119]

## II. ROLE FOR POLICYMAKERS

Policymakers at the state and federal level can help manufacturing firms better manage the multifaceted cyber threat facing smart factories. This part discusses some available reform options, beginning with civil society and insurance before moving on to standards bodies and finally to an analysis of pending bills before Congress and the importance of fostering international dialogue.

---

113. *See, e.g.*, Bernard Marr, *How Blockchain Will Transform the Supply Chain and Logistics Industry*, FORBES (Mar. 23, 2018, 12:28 AM), https://www.forbes.com/sites/bernardmarr/2018/03/23/how-blockchain-will-transform-the-supply-chain-and-logistics-industry/#1ebae465fecd (explaining the benefits and uses of blockchain technology).

114. *Id.*

115. *Id*.

116. Marr, *supra* note 113.

117. *Id*.

118. *See* Edmund Lee, *Why Blockchains Can Be Really Bad. Or: How Techno-Futurists Can Ruin Things*, RECODE (June 19, 2016), https://www.recode.net/2016/6/19/11972818/dao-hacked-blockchain-ethereum [https://perma.cc/GB7F-ZBYV] (describing how the Decentralized Autonomous Organization, a democratically controlled investment group operated on the blockchain, was hacked by exploiting vulnerabilities in its code).

119. *See* Scott J. Shackelford & Steve Myers, *Block-by-Block: Leveraging the Power of Blockchain Technology to Build Trust and Promote Cyber Peace*, 19 YALE J. L. & TECH. 334, 366–69 (2017) (explaining differences in blockchain regulatory schemes that governmental bodies have adopted).

### A. INSTILLING CYBERSECURITY RISK MANAGEMENT BEST PRACTICES: A ROLE FOR INSURANCE?

Instead of top-down regulation, many, particularly in industry, prefer self-regulation with the flexibility "to adapt to rapid technological progress."[120] Such self-regulation has the capacity to adapt better and faster than black letter law to rapidly changing technological and social forces,[121] though it is certainly not without its problems.[122] Consumer Reports is an example of an organization that is trying to create such a community. In March 2017, Consumer Reports launched its Digital Standard, which is designed "to measure the privacy and security of products, apps, and services."[123] Once it fully matures, the Digital Standard could help empower consumers to select products—including in the IoT context—that meet rigorous privacy and security requirements. Of course, Consumer Reports is not a regulatory organization, vendors will still be legally able to sell products that do not meet the Digital Standard. However, the Digital Standard might help 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. These efforts are already having an impact, the Digital Standard was instrumental in exposing privacy risks in the fertility app Glow.[124] As the Digital Standard is continually refined and

---

120. MONROE E. PRICE & STEFAAN G. VERHULST, SELF-REGULATION AND THE INTERNET 21 (2005).

121. *See id.* at 21–22 ("[S]elf-regulation offers the benefits of greater efficiency, increased incentives for compliance, and reduced cost.").

122. *See generally* 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), http://dlc.dlib.indiana.edu/dlc/bitstream/handle/10535/4417/W08-6_Ostrom_DLC.pdf (describing the advantages and disadvantages of polycentric governance).

123. *Consumer Reports Launches Digital Standard to Safeguard Consumers' Security and Privacy in Complex Marketplace*, CONSUMER REP. (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/ [https://perma.cc/Y8SF-B4QJ].

124. *See* Jerry Beilinson, *Glow Pregnancy App Exposed Women to Privacy Threats, Consumer Reports Finds*, CONSUMER REP. (July 28, 2016), https://www.consumerreports.org/mobile-security-software/glow-pregnancy

globalized, as is happening now in dialogue with the EU, it will likely further impact the trajectory and rate of global IoT privacy and security standards, including those available to manufacturers.[125]

The insurance industry is similarly helping to incentivize the uptake of cybersecurity best practices. Chris Palmer, a former Technology Director of the Electronic Frontiers Foundation has called it a "key part of the [cybersecurity] solution."[126] Although estimates vary,[127] this market could be worth more than $7.5 billion by 2020,[128] and $23.07 billion by 2025.[129] Regulatory developments, such as the Securities and

---

-app-exposed-women-to-privacy-threats/ (discussing various privacy concerns in the Glow app, as well as Glow, Inc.'s efforts to address these concerns).

125. *See* 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/ (describing the likely effect of the GDPR on U.S. consumers); 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*.").

126. Interview with Chris Palmer, Google Eng'r and former Tech. Dir., Elec. Frontiers Found., in S.F., Cal. (Feb. 25, 2011) (on file with the author).

127. *See* Nicole Perlroth, *Insurance Against Cyber Attacks Expected to Boom*, N.Y. TIMES BITS (Dec. 23, 2011, 10:58 AM), http://bits.blogs.nytimes.com /2011/12/23/insurance-against-cyber-attacks-expected-to-boom/ (noting that "[t]here are no statistics on the size of the cyber insurance industry" and discussing how the estimated "$750 million worth of premiums placed [in 2011] . . . could grow by 50 percent over the next 12 to 18 months."); *cf.* Robert Lemos, *Should SMBs Invest in Cyber Risk Insurance?*, DARK READING (Sept. 9, 2010, 5:09 PM), https://www.darkreading.com/should-smbs-invest-in-cyber -risk-insurance/d/d-id/1134322 [https://perma.cc/4GFX-H4XV] (reporting that in 2010 "companies will take out around $600 million in premiums for cyber risk . . . .").

128. *See* Jim Finkle, *Cyber Insurance Premiums Rocket After High-Profile Attacks*, REUTERS (Oct. 12, 2015, 12:33 AM), http://www.reuters.com/article /2015/10/12/us-cybersecurity-insurance-insight-idUSKCN0S609M20151012 ("[T]he cyber insurance market is set to triple to about $7.5 billion over the next five years . . . ."); *accord* PWC, INSURANCE 2020 & BEYOND: REAPING THE DIVIDENDS OF CYBER RESILIENCE 10 (2015), https://www.pwc.com/gx/en/insurance/publications/assets/reaping-dividends -cyber-resilience.pdf ("We estimate that the cyber insurance market could grow to . . . at least $7.5 billion by 2020.").

129. *See Global Cyber Security Insurance Market Size Forecast to Exceed USD 20 Billion by 2025*, ADROIT MARKET RESEARCH, (Apr. 6, 2019), https://www.adroitmarketresearch.com/press-release/cyber-security

Exchange Commission (SEC) cyber attack disclosure guidelines, could reinforce this trend.[130] Yet calculating cyber risk insurance premiums is no simple feat given the paucity of reliable data.[131] Even defining covered "cyber attacks" and cybersecurity best practices can be difficult, though an insurance company might use the NIST CSF and FTC guidelines discussed above as helpful data points.[132] Overall, the insurance industry could aid in the process of boosting cybersecurity due diligence across the economy, including in the manufacturing sector. Over time, such efforts may improve the overall level of cybersecurity preparedness of manufacturing firms, though it is important to understand that such coverage is only part of the solution, and that it is vital to review coverage terms lest patchy policies contribute to an inaccurate and reactive mindset on the part of covered firms.[133]

### B. FEDERAL POLICY OPTIONS

An array of policy options are being discussed at the federal level that would impact the growth and development of IIoT applications. This section focuses on the most recent of these efforts, including establishing baseline cybersecurity standards through an IoT security bill, protecting consumer privacy through a repackaged Privacy Bill of Rights, as well as

---

-insurance-market ("The global [c]yber security insurance market size was USD 3.89 billion in 2017 and is expected to grow to USD 23.07 billion in 2025 . . . ."). *See also 33.8%+ Growth for Cyber Insurance Market Size to 2024*, MARKETWATCH, (Feb. 8, 2019, 11:22 PM), https://www.marketwatch.com/press-release/338-growth-for-cyber-insurance-market-size-to-2024-2019-02-08 ("[T]he Cyber Insurance . . . global market size will reach US[D]16700 million by 2024 . . . .").

130. *See* Perlroth, *supra* note 127 (attributing the anticipated growth in cyber insurance premiums to the 2010 SEC disclosure guidance, among other factors).

131. *Cf.* Sarah Veysey, *Insurers Urge Anonymous Database to Help Underwrite Cyber Risks*, BUS. INS. (May 23, 2016), http://www.businessinsurance.com/article/20160523/NEWS06/160529961 ("The Association of British Insurers has called for a national anonymous database of cyber incidents to enable the insurance market to better assess, underwrite and price cyber risks.").

132. *See supra* Section 1(A)(3).

133. *See*, *e.g.*, Scott Shackelford, *Should Your Firm Invest in Cyber Risk Insurance?*, 55 BUS. HORIZONS 349, 353–55 (2012) (noting cyber insurance policies "could contribute to a more reactive focus maintaining the suboptimal cybersecurity status quo.").

encouraging proactive cybersecurity measures through allowing limited active defense.

1. Codifying Cybersecurity Baselines: Proposed IoT Security Bill

Senators Mark Warner, Cory Gardner, Ron Wyden, and Steve Daines introduced the IoT Cybersecurity Act of 2017 with this aim in mind.[134] 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," (3) that they "rely on standard protocols," and (4) they "don't contain hard-coded passwords."[135] However, the bill does not take a one-size-fits-all approach 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.[136] 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,[137] but also has its share of critics.[138] This bill has still not become law as of 2019, so perhaps other alternatives should be considered.[139] These alternatives include the Internet of Things Cybersecurity

---

134. *See generally* S. 1691, 115th Cong. pmbl., § 1 (2017) (providing for "minimal cybersecurity operational standards for [i]nternet-connected devices purchased by Federal agencies, and for other purposes."). In 2019 a modified version of the bill was reintroduced by the same sponsors. Internet of Things (IoT) Cybersecurity Act, S. 734, 116th Cong. (2019).

135. MARK WARNER ET AL., INTERNET OF THINGS CYBERSECURITY IMPROVEMENT ACT OF 2017 FACT SHEET 1 (2017), https://www.warner.senate.gov/public/_cache/files/8/6/861d66b8-93bf-4c93-84d0-6bea67235047/8061BCEEBF4300EC702B4E894247D0E0.iot-cybesecurity-improvement-act---fact-sheet.pdf.

136. *Id*.

137. *See id*. at 2.

138. *See* Brian Krebs, *New Bill Seeks Basic IoT Security Standards*, KREBS ON SEC. (Aug. 1, 2017), https://krebsonsecurity.com/2017/08/new-bill-seeks-basic-iot-security-standards/ [https://perma.cc/C238-TE8N] (criticizing the bill for "exempt[ing] cybersecurity researchers engaging in good-faith research from liability under the Computer Fraud and Abuse Act and the Digital Millennium Copyright Act when in engaged in research pursuant to adopted coordinated vulnerability disclosure guidelines.").

139. *See S. 1691: Internet of Things (IoT) Cybersecurity Improvement Act of 2017 Track S. 1691*, GOVTRACK, https://www.govtrack.us/congress/bills/115/s1691 (last visited Dec. 20, 2019).

Improvement Act of 2019, which calls upon NIST and the Office of Management and Budget (OMB) to "leverage Federal Government procurement power to encourage increased cybersecurity for Internet of Things devices."[140]

2. Protecting Consumer Privacy: Privacy Bill of Rights

There are proposals at the federal level, similar to California's 2018 Consumer Privacy Act. These proposals seek to codify some of the protections similar to the protections in the GDPR, discussed above. This Privacy Bill of Rights, a version of which was first trumpeted by the Obama Administration in 2012, was part of the CONSENT (Consumer Online Notification for Stopping Edge-provider Network Transgressions) Act introduced by Senate Democrats in 2018 in the wake of the Cambridge Analytica scandal.[141] If enacted, the law would require covered firms "to obtain opt-in consent from users before sharing, selling or otherwise using their personal information . . . [along with] develop[ing] reasonable data security practices."[142] It would impact manufacturers directly since its cybersecurity and data processing requirements would apply not just to social networks, but to an array of publicly traded firms including those deploying IIoT tech.[143]

---

140. Micha Nandaraj Gallo, *Senate Reintroduces IoT Cybersecurity Improvement Act*, INSIDE PRIVACY (Mar. 12, 2019), https://www.insideprivacy.com/internet-of-things/senate-reintroduces-iot-cybersecurity-improvement-act/.

141. *See* Marguerite Reardon, *Senate Dems Introduce 'Privacy Bill of Rights*,' CNET (Apr. 10, 2018 11;58 AM), https://www.cnet.com/news/senate-dems-introduce-privacy-bill-of-rights/ (describing the CONSENT Act introduced to "establish privacy protections for people who use online platforms, like Facebook and Google.").

142. *Id*.

143. *See* S. 2639, 115th Cong. (2017) (the bill applies to all providers of "edge services" defined within the bill as services provided over the internet which require a subscription "through which a program searches for and identifies items in a database that correspond to keywords or characters specified by the customer" which could conceivably affect many manufacturers).

3. Fostering Proactive Cybersecurity: Active Defense Bill

In 2018, Congress considered a wide range of cybersecurity legislation from a privacy bill of rights[144] to election security.[145] Relevant to this discussion, they also considered a version of the Active Cyber Defense Certainty (ACDC) Act.[146] The ACDC Act[147] would permit firms to operate beyond their network perimeter, including the potential to conduct surveillance on entities "who are thought to have done hacking in the past or who, according to a tip or some other intelligence, are planning an attack."[148] The bill also clarifies "the type of tools and techniques that defenders can use that exceed the boundaries of their own computer network."[149] In summary, according to Congressman Graves, "[t]his is an effort to give the private sector the tools they need to defend themselves."[150] If enacted, such a policy would allow manufacturers to potentially target foreign sponsors of cyber attacks.[151]

---

144. *See* Press Release, Ed Markey, U.S. Senator for Mass., As Facebook CEO Zuckerberg Testifies to Congress, Senators Markey and Blumenthal Introduce Privacy Bill of Rights (Apr. 10, 2018), https://www.markey.senate.gov/news/press-releases/as-facebook-ceo-zuckerberg-testifies-to-congress-senators-markey-and-blumenthal-introduce-privacy-bill-of-rights (aiming to "protect the personal information of American consumers"). Specifically, Markey and Blumenthal introduced the bill to: "Require[] edge providers to obtain opt-in consent from users to use, share, or sell users' personal information[,] . . . to develop reasonable data security practices[,] . . . to notify users about all collection, use, and sharing of users' personal information[,] . . . [and] to notify users in the event of a breach[.]" *Id.*

145. *See* Martin Matishak, *Lawmakers Gather Behind Election Security Bill — At Last*, POLITICO (Mar. 22, 2018, 10:42AM), https://www.politico.com/story/2018/03/22/election-security-bill-congress-437472 (describing congressional efforts to pass the Secure Elections Act).

146. Active Cyber Defense Certainty Act, H.R. 4036, 115th Cong. (2017).

147. *Id. See, e.g.*, Patrick Howell O'Neill, *Rep. Graves: 'Active Defense' Bill Will Launch a New Industry*, CYBERSCOOP (Nov. 27, 2017), https://www.cyberscoop.com/tom-graves-active-defense-hack-back-bill-new-industry/ (reporting that the bill attracted both support and criticism).

148. Nicholas Schmidle, *The Digital Vigilantes Who Hack Back*, NEW YORKER (Apr. 30, 2018), https://www. newyorker.com/magazine/2018/05/07/the-digital-vigilantes-who-hack-back.

149. H.R. 4036, 115th Cong. § 2(11) (2017).

150. Schmidle, *supra* note 148.

151. *See* Tom Kulik, *Why the Active Cyber Defense Certainty Act Is a Bad Idea*, ABOVE THE LAW (Jan. 29, 2018, 17:30 PM), https://abovethelaw.com/2018/01/why-the-active-cyber-defense-certainty-act-is-a-bad-idea/ [https://perma.cc/4L37-UCMG] (noting that the ACDC Act would allow a company to defend against attackers including those outside the United States).

Concerns regarding the ACDC act, though, fall across several dimensions. Some, such as former National Security Agency Directors Admiral Michael S. Rogers and Keith Alexander, are concerned about further complicating an already complex cyber threat landscape.[152] Others, such as Rob Joyce, President Trump's cybersecurity adviser, are more concerned about sanctioning "vigilantism" which could, he argued, even in a best-case scenario, lead to "unqualified actors bringing risk to themselves, their targets, and their governments."[153] A new version of the Act was introduced in 2019.[154]

In general, there is a growing consensus that firms should practice *passive* defense best practices,[155] and not "hacking back" to recover assets due to serious concerns regarding attribution and escalation.[156]

### C. GOVERNING SMART FACTORIES AND OPPORTUNITIES FOR NORMS DEVELOPMENT

There are many ways to conceptualize cybersecurity policy in the IIoT context, but among them is the dynamic field of polycentric governance.[157] As this author has described it previously, this governance framework may be considered to be a multi-level, multi-purpose, multi-functional, and multi-sectoral model,[158] championed by numerous scholars including

---

152. *See* Schmidle, *supra* note 148.

153. *Id*.

154. Active Cyber Defense Certainty Act, H.R. 3270, 116th Cong. (2019). *See* Robert Chesney, *Hackback Is Back: Assessing the Active Cyber Defense Certainty Act*, LAWFARE (June 14, 2019), https://www.lawfareblog.com/hackback-back-assessing-active-cyber-defensecertainty-act [https://perma.cc/MA45-KWC3] (explaining the new version's provisions).

155. *See id.* at 9 fig. 1 (illustrating the spectrum of cyber defense).

156. *See id.* at 5 (explaining the unintended consequences of certain active cyber defense measures).

157. 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.").

158. *See id.* at 171–72 (explaining the characteristics of polycentric governance).

Nobel Laureate Elinor Ostrom and Professor Vincent Ostrom.[159] It "challenges orthodoxy [in part] by demonstrating the benefits of self-organization and networking regulations '*at multiple scale*s.'"[160] Rather than attempting a unitary response to managing "global collective action problems,"[161] such as cyber-attacks, 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.'"[162] This, in other words, envisions an all-of-the-above approach that harnesses positive network effects that could, in time, result in the emergence of a "norm cascade" improving smart factory security.[163] Moreover, the various analytical tools developed to help measure and implement the findings from the polycentric governance literature, including the Ostrom Design Principles and the Institutional Analysis and Development (IAD) Framework,[164] may help create an analytical guide for smart factories to identify governance gaps.[165]

One example of a successful public-private polycentric collaboration is the NIST CSF, which, as has been noted, is now

---

159. *See* 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), http://dlc.dlib.indiana.edu /dlc/bitstream/handle/10535/4417/W08-6_Ostrom_DLC.pdf (reviewing "studies of polycentric governance systems in metropolitan areas and for managing common-pool resources.").

160. *See* Scott J. Shackelford, *Toward Cyberpeace: Managing Cyber Attacks Through Polycentric Governance*, 62 AM. U. L. REV. 1273, 1283 (2013).

161. Elinor Ostrom, *A Polycentric Approach for Coping with Climate Change*, 15 ANNALS ECON. & FIN. 97, 97 (2014).

162. Shackelford, *supra* note 160, at 1284 (quoting 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[.]").

163. Martha Finnemore & Kathryn Sikkink, *International Norm Dynamics and Political Change*, 52 INT'L ORG. 887, 895 (1998); *see id.* at 895–99 (explaining the three-stage norm life cycle including "norm emergence," "norm cascade," and "norm internalization").

164. *See generally* Elinor Ostrom, *Background on the Institutional Analysis and Development Framework*, 39 POL'Y STUD. J. 7 (2011).

165. For more on this topic, see SCOTT J. SHACKELFORD & AMANDA N. CRAIG DECKARD, THE INTERNET OF EVERYTHING: WHAT EVERYONE NEEDS TO KNOW (forthcoming 2019).

going global.[166] The success of such frameworks, civil society efforts like the Consumer Reports Digital Standard,[167] and regional regimes like the EU General Data Protection Regulation,[168] is part and parcel of the literature on polycentric governance given the extent to which it leverages self-organization while also recognizing the need for a coordinating function between disparate groups and governance scales.[169] 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.[170] The Ostrom Design Principles referenced above can help predict the institutional success of given interventions.[171] Still, the literature remains immature, as does the current state of IoT governance. In fact, the ISACA, previously known as the Information Systems Audit and Control Association,[172] 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."[173]

---

166. *See* NAT'L INST. OF STANDARDS & TECH., *supra* note 53 (introducing and explaining the framework).

167. *See* Press Release, Consumer Reports, Consumer Reports Launches Digital Standard to Safeguard Consumers' Security and Privacy in Complex Marketplace (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/ (introducing the Digital Standard).

168. Commission Regulation 2016/679 of Apr. 27, 2016, General Data Protection Regulation, 2016 O.J. (L 119).

169. *See generally* Ostrom, *supra* note 159 ("Solving collective-action problems requires opening public and private spheres of activities ranging from the small to the very large so as to encourage effective problem solving.").

170. *See* Robert O. Keohane & David G. Victor, *The Regime Complex for Climate Change*, 9 PERSP. ON POL. 7, 15 (2011) ("Components may conflict with one another in ways that yield gridlock rather than innovation; the lack of hierarchy among specific regimes can create critical veto points. . . .").

171. *See generally* Shackelford et al., *supra* note 8.

172. *About ISACA*, ISACA, http://www.isaca.org/about-isaca/Pages/default.aspx (last visited Dec. 20, 2019).

173. *Existing Security Standards Do Not Sufficiently Address IoT*, HELP NET SECURITY (Oct. 15, 2015), http://www.net-security.org/secworld.php?id=18981 [https://perma.cc/SXZ2-KX32].

Manufacturing firms should engage in these conversations. Manufacturing firms have already made considerable progress in making attacks on civilian critical infrastructure, including smart factories, off limits. They have also made considerable investments in both security and privacy by design, but they can go farther by refining the scope. This involves further refining the scope of cybersecurity due diligence at the international level, as well as boosting public-private information sharing, and even recasting the cybersecurity debate in the manufacturing sector as not just an exercise in cost-benefit analysis, but as a corporate social responsibility. Firms could build from this conception by participating in communities to help spread this approach, such as through the Cybersecurity Tech Accord,[174] and the Paris Call for Trust and Security in Cyberspace.[175]

## CONCLUSION

As the IoT matures, and more things and organizations are connected, there is a potential to build smart (and potentially more resilient) things, factories, and societies. Smart factories and their impacts span myriad sectors and industries. In response, polycentric IoT governance systems should be leveraged to improve critical infrastructure security and protect consumer privacy.[176] This includes frameworks and standards—including an 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 smart factories as part of improving security and data privacy in the ever-expanding Internet of Everything.

---

174. *See* James Sanders, *Cybersecurity Tech Accord Sets New Privacy Standards for Tech Companies*, TECHREPUBLIC. (Apr. 18, 2018), https://www.techrepublic.com/article/cybersecurity-tech-accord-sets-new-privacy-standards-for-tech-companies/.

175. *See* Louise Matsakis, *The US Sits out an International Cybersecurity Agreement*, WIRED (Nov. 12, 2018), https://www.wired.com/story/paris-call-cybersecurity-united-states-microsoft/ [https://perma.cc/GXD5-B9LK].

176. *See* Shackelford, *supra* note 160 at 1286.