NEW YORK LAW SCHOOL

NYLS Law Review
Vols. 22-63 (1976-2019)

Volume 62
Issue 2 *Exploring the Things in the Internet of Things: Implications For Business, Consumers, and the Law*

Article 2

January 2018

The Industrial Internet of Things: Risks, Liabilities, and Emerging Legal Issues

Mauricio Paez

Kerianne Tobitsch

VOLUME 62 | 2017/18

MAURICIO PAEZ AND KERIANNE TOBITSCH

The Industrial Internet of Things: Risks, Liabilities, and Emerging Legal Issues

62 N.Y.L. Sch. L. Rev. [•] (2017–2018)

ABOUT THE AUTHOR: Mauricio Paez is a partner and Kerianne Tobitsch is an associate in the New York office of Jones Day; they are members of the firm's Global Cybersecurity, Privacy & Data Protection Group. The authors thank Steven W. Magnusson, an associate at the firm, for assisting with the research for this work. The views expressed in this article are solely that of the authors and not of Jones Day or its other partners.

I. THE "INDUSTRIAL INTERNET OF THINGS": BACKGROUND

The industrial Internet of Things ("IoT") has the promise to revolutionize the industrial sector in the United States and around the world. While much of the focus has been on the consumer IoT,[1] the industrial IoT is estimated to grow close to 100 billion connected devices in the next five years and will likely outpace the consumer IoT due to the large-scale nature of the industrial products sector.[2] Almost every industrial sector has the ability to leverage sensors and other technologies to generate insight from industrial equipment by collecting and analyzing data in real time.[3] The industrial IoT is expected to have a transformational effect on the industrial sector by changing the way industries innovate, collaborate, and create new efficiencies by leveraging big data analytics, artificial intelligence, and virtual collaboration to derive business insight.

The industrial IoT, sometimes called the Industrial Internet or Industry 4.0,[4] refers to the digital transformation of the industrial sector.[5] Though there is no universal definition of the industrial IoT, it generally refers to the proliferation of industrial systems, machines, and devices capable of interacting with the physical environment, people, and other devices.[6] Electronic sensors,[7] industrial internet

1. The consumer Internet of Things refers to everyday consumer products embedded with technology that enables those products to interact with the physical environment, people, and other devices. Mauricio Paez & Mike La Marca, *The Internet of Things: Emerging Legal Issues for Businesses*, 43 N. Ky. L. Rev. 29, 31–32 (2016).

2. PricewaterhouseCoopers, The Industrial Internet of Things 7 (2016), https://www.pwc.com/gx/en/technology/pdf/industrial-internet-of-things.pdf; *see also* Paez & La Marca, *supra* note 1, at 32–34.

3. Gen. Elec. Co. & Accenture, Industrial Internet Insights Report 7 (2015) [hereinafter Industrial Internet Insights Report], https://www.ge.com/digital/sites/default/files/industrial-internet-insights-report.pdf.

4. *See, e.g.*, *About Us*, Indus. Internet Consortium, http://www.iiconsortium.org/working-committees.htm (last visited Apr. 1, 2018); Cornelius Baur & Dominik Wee, *Manufacturing's Next Act*, McKinsey & Company: Insights on Operations (June 2015), https://www.mckinsey.com/business-functions/operations/our-insights/manufacturings-next-act; *What is the Industrial Internet of Things?*, Gen. Electric Company, https://www.ge.com/digital/blog/everything-you-need-know-about-industrial-internet-things (last visited Apr. 1, 2018).

5. *See generally* Brian Hartmann, William P. King, & Subu Narayanan, *Digital Manufacturing: The Revolution Will Be Virtualized*, McKinsey & Company: Insights on Operations (Aug. 2015), https://www.mckinsey.com/business-functions/operations/our-insights/digital-manufacturing-the-revolution-will-be-virtualized ("[T]he explosion in data and new computing capabilities—along with advances in other areas such as artificial intelligence, automation and robotics, additive technology, and human-machine interaction—are unleashing innovations that will change the nature of manufacturing itself.").

6. *See* Paez & La Marca, *supra* note 1, at 31.

7. An electronic sensor is a device designed to detect, measure, or respond to an input from the environment in which it is operating, such as "light, heat, motion, moisture, pressure, or any one of a great number of other environmental phenomena." *Sensor*, TechTarget & WhatIs.com, https://whatis.techtarget.com/definition/sensor (last updated July 2012); *50 Sensor Applications for a Smarter World*, Libelium, http://www.libelium.com/resources/top_50_iot_sensor_applications_ranking/ (last visited Apr. 1, 2018) (listing various smart devices that interact with the physical environment to, for example, detect air pollution, measure water pressure, and help predict forest fires).

software, or other embedded technologies[8] generate and transmit data from these devices over an internet-connected network.[9] Companies can then analyze the data, which is often stored in cloud applications, to guide decision-making, improve safety and organizational processes, reduce waste, promote efficiency, and lessen environmental impact.[10]

There is enormous potential for growth in almost all industries through development of industrial IoT applications, as almost anything can be made into an intelligent machine.[11] The industrial IoT has already been leveraged in a range of asset-heavy industries, including manufacturing, logistics, mining, oil and gas, utilities, and agriculture.[12] Data generated by industrial equipment holds enormous business value.[13] For example, attaching sensors to the machinery on a factory floor generates data about inventory flows, production levels, and machinery performance, which allows a company to optimize factory operations by adjusting machinery and operational decisions as needed in response to the data.[14] In the transportation sector, sensors attached to trucks can "collect data on fuel consumption, tire pressure, temperature, speed and location."[15] The industrial IoT is having a profound impact on the oil and gas industry, which has incorporated some of the most advanced applications of the industrial IoT to date.[16] Unlike the manufacturing industry, where processes are performed in the closed setting of a factory, the outdoor operating environment in the oil and gas industry presents additional challenges to productivity, reliability of equipment, predictability of working conditions, complexity of supply chains, and maintenance of asset integrity.[17] To address these challenges, new

8. An embedded computer technology is a "special-purpose system in which the computer is completely encapsulated by the device it controls." Dep't of Elec. & Comput. Eng'g, *Embedded Computer Systems*, N.C. St. U., https://www.ece.ncsu.edu/research/cas/ecs (last visited Apr. 1, 2018).

9. Paez & La Marca, *supra* note 1, at 31.

10. *Id.*

11. Paul Daugherty et al., Accenture, Driving Unconventional Growth Through the Industrial Internet of Things 11 (2015), https://www.accenture.com/us-en/_acnmedia/Accenture/next-gen/reassembling-industry/pdf/Accenture-Driving-Unconventional-Growth-through-IIoT.pdf.

12. *The Industrial IoT: 125+ Startups Transforming Factory Floors, Oil Fields, and Supply Chains*, CB Insights: Research (May 5, 2017), https://www.cbinsights.com/research/top-startups-iiot/ [hereinafter CB Insights].

13. *Id.*; *e.g.*, Bhoopathi Rapolu, *Internet of Aircraft Things: An Industry Set to Be Transformed*, Aviation Wk. Network (Jan. 18, 2016), http://aviationweek.com/connected-aerospace/internet-aircraft-things-industry-set-be-transformed (discussing the immense business value the industrial IoT is expected to have in the aircraft industry).

14. James Manyika et al., McKinsey Glob. Inst., The Internet of Things: Mapping the Value Beyond the Hype 66 (2015), https://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/the-internet-of-things-the-value-of-digitizing-the-physical-world (follow "Full Report (PDF–3MB)").

15. Daugherty et al., *supra* note 11, at 8.

16. Manyika et al., *supra* note 14, at 74.

17. *Id.*

production platforms in the oil and gas industry have up to thirty thousand sensors to generate real-time data and adjust production strategy.[18]

The industrial IoT enables industrial companies to improve operational efficiency and optimize assets and operations, and ultimately may affect profitability and alter the competitive landscape.[19] Even a small increase in productivity could generate billions of dollars a year.[20] Failure to embrace the industrial IoT may mean the failure of an industrial company to remain competitive in the future.[21] Conservative estimates place the expected global economic impact of the industrial IoT at $500 billion of GDP by 2020.[22] Other estimates of the industrial IoT's value reach up to $15 trillion of global GDP by 2030.[23] To capture this full economic value, there will need to be innovation in organizational management, business models, and technical standards,[24] all of which will present risks, potential liabilities, and emerging legal issues. Part II of this article discusses the cybersecurity risks inherent in the industrial IoT, related liabilities, and potential approaches to mitigate these risks. Part III discusses the need to obtain intellectual property protection and the obstacles faced when doing so. Part IV addresses the technical and legal challenges to achieving the degree of interoperability necessary for the industrial IoT to achieve its full potential, as well as potential licensing solutions. Part V focuses on the legal challenges and risks arising in certain industrial sectors with early adoption of the industrial IoT. Part VI addresses the aggressive data protection regime emerging in the European Union and the regulatory compliance implications for industrial IoT companies. Part VII concludes this article.

II. SECURITY RISKS PRESENT POTENTIAL LEGAL LIABILITIES

Greater connectivity of operational technology exposes a company's operations to security risks.[25] Cyberattacks against industrial companies have increased in recent years,

18. *Id.*; *see also* Riccardo Bertocco & Vishy Padmanabhan, Bain & Co., Big Data Analytics in Oil and Gas 1 (2014), http://www.bain.com/Images/BAIN_BRIEF_Big_Data_analytics_in_oil_and_gas.pdf (discussing the benefits of utilizing big data analytics generated by sensors in the oil and gas industry).

19. Industrial Internet Insights Report, *supra* note 3, at 10.

20. Daugherty et al., *supra* note 11, at 4.

21. *See* European Comm'n, *Communication from the Commission on Standard Essential Patents for a European Digitalised Economy*, at 1, Ref. Ares (2017)1906931 (Oct. 4, 2017) [hereinafter EC Roadmap], https://ec.europa.eu/info/law/better-regulation/initiatives/ares-2017-1906931_en (follow "Download"); *see also* Matt Loeb, *Internet of Things Security Issues Require a Rethink on Risk Management*, Wall Street J.: CIO J. (Oct 14, 2015, 12:32 PM), https://blogs.wsj.com/cio/2015/10/14/internet-of-things-security-issues-require-a-rethink-on-risk-management/ (arguing that the benefit of embracing the IoT outweighs security risks that come along with it).

22. Daugherty et al., *supra* note 11, at 4.

23. *Id.*

24. Manyika et al., *supra* note 14, at 2.

25. Ivan Fernandez, Frost & Sullivan & Schneider Elec., Cybersecurity for Industrial Automation & Control Environments 3 (2013), https://download.schneider-electric.com/files?p_enDocType=White+Paper&p_File_Id=1165513224&p_File_Name=998-2095-04-13-13AR0_EN.PDF&p_Reference=998-2095-04-13-13AR0_EN; Rene Millman, *Cybersecurity Attacks on IIoT*

and the incidence of malicious attacks is expected to rise in the future.[26] Cyberattacks on industrial control systems in particular are a significant challenge for industrial companies and occur with increasing frequency.[27] Attacks on a control system can disrupt industrial activity on a large scale because the control system is the nerve center of an industrial environment.[28] A cyberattack on a control system even has the potential to cause physical damage to an industrial system.[29] For example, in 2014, a cyberattack against a German steel mill caused significant physical damage to the mill when hackers took over the control system and prevented a blast furnace from shutting down.[30]

A. Security Vulnerabilities of Industrial IoT Technologies Are Unique.

The unique characteristics of the industrial IoT heightens the security challenges of digitizing an industrial environment. The sheer number of industrial IoT technologies required to digitize an industrial system itself creates a security challenge.[31] With thousands of sensors and other connected technologies deployed in an industrial environment, there are numerous access points for an outside actor to exploit.[32] The more digitalization there is in an industrial environment, the greater the risk of exposure to cyberattacks.[33]

Infrastructure Expected to Increase This Year, Internet Bus. (Mar. 13, 2017), https://internetofbusiness.com/cybersecurity-iiot-infrastructure/.

26. *See* Steve Morgan, *The Top 5 Industries at Risk of Cyber-Attacks* (May 13, 2016), https://www.forbes.com/sites/stevemorgan/2016/05/13/list-of-the-5-most-cyber-attacked-industries/#71d26b41715e. According to a recent survey of IT security professionals worldwide, ninety-six percent of respondents expect to see an increase in security attacks on industrial IoT infrastructure, but over half of respondents report that they are not prepared for malicious attacks targeting industrial IoT systems. Ray Lapena, *More than 90% of IT Pros Expect More Attacks, Risk, and Vulnerability with Industrial IoT in 2017*, Tripwire: St. Security (Mar. 13, 2017), https://www.tripwire.com/state-of-security/featured/90-pros-expect-attacks-risk-vulnerability-iiot-2017/.

27. Warwick Ashford, *Industrial Control Systems: What Are the Security Challenges?*, ComputerWeekly.com (Oct. 14, 2014, 4:58 PM), http://www.computerweekly.com/news/2240232680/Industrial-control-systems-What-are-the-security-challenges.

28. *See* Joseph Abrenio et al., *Cyber Security and the Grid: We'll Leave the Lights On For You (If We Can)*, 33 Syracuse J. Sci. & Tech. L. 3, 11 (2017).

29. *See Cyberattack on a German Steel-Mill*, Sentryo (May 31, 2017), https://www.sentryo.net/cyberattack-on-a-german-steel-mill/; 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/.

30. *Cyberattack on a German Steel-Mill*, *supra* note 29; Zetter, *supra* note 29. The hackers first gained access to the office software network of the industrial site and from there were able to penetrate the production management software for the mill. *Cyberattack on a German Steel-Mill*, *supra* note 29; Zetter, *supra* note 29.

31. *See* Scott J. Shackelford & Scott Russell, *Above the Cloud: Enhancing Cybersecurity in the Aerospace Sector*, 10 Fla. Int'l U. L. Rev. 635, 640–41 (2015).

32. *Id.*; Karen Rose et al., Internet Soc'y, The Internet of Things: An Overview 32 (2015), https://www.internetsociety.org/wp-content/uploads/2017/08/ISOC-IoT-Overview-20151221-en.pdf.

33. Shackelford & Russell, *supra* note 31, at 640–41.

Furthermore, connected technologies often have no clear way to alert a user when there is a security breach, which may allow a breach to continue for a long period without detection.[34] The risk is greater with the industrial IoT because there are simply more opportunities to exploit security vulnerabilities in an industrial environment, which deploys hundreds of connected technologies that a company could not possibly monitor on a constant basis.[35] We have already seen an example of the potentially widespread reach of a cyberattack targeting connected devices. In September 2016, a type of malware called Mirai began infecting IoT devices, enabling cybercriminals to control the devices remotely and conduct distributed denial of service (DDoS) attacks by flooding internet servers with malicious traffic to shut them down.[36] This malware affected hundreds of thousands of IoT devices in numerous countries.[37] Mirai was difficult to contain because users did not detect its presence when the malware did not noticeably affect performance of the devices.[38]

Interoperability expands the potential scope of a data breach.[39] An open and connected industrial environment means that malware or another security weakness in one device could spread quickly to other connected devices in the same network and impact the entire industrial system.[40] The seamless communication and processing of information through sensors, transmitters, and other industrial IoT technologies by nature increases the risk of spreading the damage from cyberattacks.[41]

Compounding the security challenge is that an industrial system tends to deploy identical devices.[42] While this homogeneity may improve interconnectedness, a single security vulnerability could have an outsized impact on an industrial system deploying other devices with similar design characteristics.[43] If hackers figure out how to breach the features of one device, there may be hundreds or thousands of

34. Rose et al., *supra* note 32, at 35.

35. *See* Lily Hay Newman, *The Botnet that Broke the Internet Isn't Going Away*, Wired (Dec. 9, 2016, 7:00 AM), https://www.wired.com/2016/12/botnet-broke-internet-isnt-going-away/.

36. *Id.*

37. Jason Christman, *How the Industrial Internet of Things Impacts Data and Privacy*, Honeywell, https://www.honeywell.com/newsroom/news/2017/01/how-the-industrial-internet-of-things-impacts-data-and-privacy (last updated Jan. 27, 2017).

38. Newman, *supra* note 35.

39. Manyika et al., *supra* note 14, at 105.

40. *See* Shackelford & Russell, *supra* note 31, at 640–41; Fernandez, *supra* note 25, at 3.

41. Shackelford & Russell, *supra* note 31, at 640; Manyika et al., *supra* note 14, at 105.

42. Rose et al., *supra* note 32, at 34.

43. *Id.* ("For example, a communication protocol vulnerability of one company's brand of Internet-enabled light bulbs might extend to every make and model of device that uses that same protocol or which shares key design or manufacturing characteristics."); *see, e.g.*, Liam O Murchu, *Stuxnet P2P Component*, Symantec (Sept. 17, 2010), https://www.symantec.com/connect/blogs/stuxnet-p2p-component (demonstrating how malware is easily transmitted between connected devices); Kim Zetter, *How Digital Detectives Deciphered Stuxnet, the Most Menacing Malware in History*, Wired (July 11, 2011, 7:00 AM), https://www.wired.com/2011/07/how-digital-detectives-deciphered-stuxnet/ (discussing how the Stuxnet malware targeted and disabled thousands of centrifuges at a nuclear facility in Iran).

identical devices deployed throughout an industrial system that could become vulnerable to unauthorized access.[44] The danger of homogeneity is even greater when identical devices are used in operations at multiple locations.[45] Once hackers have determined how to access industrial IoT technologies in one location, they can breach identical technologies in other locations.[46]

When industrial IoT devices are accessible outside of a protected environment, the risks are even higher. While some industries may be able to deploy industrial IoT technologies in a controlled environment, such as a manufacturing plant, other industries must use them in an open environment where they have less ability to monitor conditions.[47] For example, sensors could be attached to trucks to monitor for repairs, water meters to monitor water usage levels, or oil wells to measure temperature, pressure, and oil extraction rates.[48] The location of these technologies in an open industrial environment makes physical security difficult, exposing these technologies to unauthorized physical access and tampering.[49]

Yet another security challenge particular to the industrial IoT is the enormous amount of data stored in one place. The hundreds or thousands of connected technologies deployed across an industrial system can generate massive streams of data.[50] But collecting the data is only part of the promise of the industrial IoT. To create value for industries, this data must be stored and analyzed, and often it is stored in cloud platforms.[51] While the decreasing cost of cloud storage is enabling a wider range of industrial IoT applications,[52] storing valuable commercial data in the cloud makes an attractive target for cybercriminals or competitors looking to access sensitive or proprietary industrial data.[53]

---

44. Richard Kam, *Time to Get Security Smart About the Internet of Things*, IAPP: Privacy Advisor (Nov. 24, 2015), https://iapp.org/news/a/time-to-get-security-smart-about-the-internet-of-things/.

45. *See* Mission Support Ctr., Idaho Nat'l Lab., Cyber Threat and Vulnerability Analysis of the U.S. Electric Sector 24–25 (2016) [hereinafter Mission Support Center Analysis Report], https://www.energy.gov/sites/prod/files/2017/01/f34/Cyber%20Threat%20and%20Vulnerability%20Analysis%20of%20the%20U.S.%20Electric%20Sector.pdf ("[I]f more than one plant uses the same configuration of equipment and with the same access controls, all plants are at risk if a cyber attacker discovers a way to compromise the equipment.").

46. *Id.*

47. *See* Manyika et al., *supra* note 14, at 74.

48. *Id.*

49. Rose et al., *supra* note 32, at 34.

50. Daugherty et al., *supra* note 11 (explaining that General Electric's latest locomotive has 250 sensors that generate 150,000 data points per minute).

51. Rose et al., *supra* note 32, at 23; *see also* Manyika et al., *supra* note 14, at 17; Gen. Elec., Predix: The Industrial Internet Platform 6 (2016), https://www.ge.com/uk/sites/www.ge.com.uk/files/Predix-The-Industrial-Internet-Platform-Brief.pdf.

52. Manyika et al., *supra* note 14, at 17.

53. Thomas Barrabi, *Why Hackers Love the Cloud*, Fox Bus. (Jan. 17, 2017), http://www.foxbusiness.com/features/2016/12/16/why-hackers-love-cloud.html; Scott Nonaka & Kevin Rubino, *Contracting in the*

The prevalence of legacy systems in an industrial environment creates yet another security challenge. Many companies keep older, or "legacy," industrial equipment in use for decades so as long as those items continue to function because replacing or upgrading equipment can be costly and disruptive.[54] For this reason, companies tend to layer industrial IoT applications on top of their existing legacy systems rather than replace them.[55] As a result, an industrial environment may have both new technology and legacy machines, and industrial IoT technologies need to find a way to connect across them all.[56] These legacy systems are harder to secure because they often have limited or no security built into them[57] and are not designed for connectivity.[58]

Exploitation of the industrial IoT's security challenges could have potentially devastating consequences. On one end of the spectrum, a cyberattack or non-malicious malfunction in a connected system could cause business disruptions because a delay to even one part of a connected system can impact performance in another part.[59] A business disruption may only affect a single company, or it could cause large-scale economic harm if it impacts critical infrastructure.[60]

The consequences of a malfunction or cyberattack on a connected system could transcend mere business disruption. Industrial IoT technologies are used to manage critical systems in sensitive industries—including the management of power grids, water treatment plants, chemical facilities, hospitals, and financial networks[61]—which multiplies the security risks because a disturbance has the potential to disrupt

---

Cloud: Who Pays for a Data Breach?, Bloomberg BNA (Oct. 18, 2016), https://www.bna.com/contracting-cloud-pays-n57982078761/.

54. Rose et al., *supra* note 32, at 49; Ashford, *supra* note 27; Bernard Marr, *Unlocking the Value of the Industrial Internet of Things (IIoT) and Big Data in Manufacturing*, Forbes (April 21, 2017, 12:35 AM), https://www.forbes.com/sites/bernardmarr/2017/04/21/unlocking-the-value-of-the-industrial-internet-of-things-iiot-and-big-data-in-manufacturing-2/#66ebeb176861.

55. Paez & La Marca, *supra* note 1, at 46.

56. *See* Marr, *supra* note 54.

57. Daugherty et al., *supra* note 11, at 13.

58. Ashford, *supra* note 27.

59. Nick Kostov & Costas Paris, *Companies Try to Contain Fallout from Global Cyberattack*, Wall Street J. (June 28, 2017, 5:27 PM), https://www.wsj.com/articles/fallout-from-global-cyberattack-extends-into-second-day-1498639146.

60. Manyika et al., *supra* note 14, at 105. For example, a software bug in the North American electric grid in 2003 led to widespread electrical power outages that disrupted businesses, utilities, transportation, and cell phone service for two days in several northeastern and midwestern states and parts of Canada. James Barron, *The Blackout of 2003: The Overview; Power Surge Blacks Out Northeast, Hitting Cities in 8 States and Canada; Midday Shutdowns Disrupt Millions*, N.Y. Times (Aug. 15, 2003), http://www.nytimes.com/2003/08/15/nyregion/blackout-2003-overview-power-surge-blacks-northeast-hitting-cities-8-states.html; Hugh Byrd and Steve Matthewman, *Lights Out: The Dark Future of Electric Power*, New Scientist (May 7, 2014), https://www.newscientist.com/article/mg22229684-300-lights-out-the-dark-future-of-electric-power/; *see generally* N. Am. Elec. Reliability Council, Technical Analysis of the August 14, 2003 Blackout (2004), http://www.nerc.com/docs/docs/blackout/NERC_Final_Blackout_Report_07_13_04.pdf.

61. Zetter, *supra* note 29.

critical services to citizens.[62] Interference with industrial IoT technologies that manage the physical world, such as the breach of a water system, hospital equipment, chemical facility, or other regulated utility, could place public health and safety at risk when those technologies are directed to behave in unpredictable or undesirable ways.[63] For example, in 2016, hackers reportedly gained access to the control system at a water utility and changed the levels of chemicals used to treat tap water by manipulating the valves controlling the flow of the chemicals.[64]

B. Legal Exposure from Cybersecurity Incidents

The challenge of securing a vast and integrated industrial system presents potential liability risks. In the event of a data breach, an industrial company could face one or more of the following: potential litigation, contractual liability, and regulatory enforcement. The steps a company takes to address security concerns before an incident occurs could impact the scope of the company's liability. Industrial companies must address security vulnerabilities even though guidance, standards, and case law surrounding data security liabilities are still developing.

Companies may face litigation risk related to their security practices in the event of a data breach. Litigants have tried a variety of claims, with mixed success, to recover losses arising from data breaches.[65] Negligence claims in particular present a risk of liability because some plaintiffs have been successful in stating a claim for negligence and surviving a motion to dismiss.[66] Some courts have recognized a duty to exercise reasonable care in safeguarding certain categories of data,[67] though this is a developing

62. Manyika et al., *supra* note 14, at 105. For example, in December 2015, hackers gained control of a power grid in Ukraine and remotely opened circuit breakers, causing swift and widespread power outages for up to 230,000 citizens. Andrew Roth, *Not Just the DNC: Five More Hacks the West Has Tied to Russia*, Wash. Post (June 15, 2016), https://www.washingtonpost.com/news/worldviews/wp/2016/06/15/not-just-the-dnc-five-more-hacks-the-west-has-tied-to-russia/?utm_term=.5731e95bb427.

63. *See* Manyika et al., *supra* note 14, at 105; Zetter, *supra* note 29.

64. John Leyden, *Water Treatment Plant Hacked, Chemical Mix Changed for Tap Supplies*, Register (Mar. 24, 2016, 12:19 PM), https://www.theregister.co.uk/2016/03/24/water_utility_hacked/; Eduard Kovaks, *Attackers Alter Water Treatment Systems in Utility Hack: Report* (Mar. 22, 2016), https://www.securityweek.com/attackers-alter-water-treatment-systems-utility-hack-report. The operational technology at the utility reportedly ran on an outdated system, highlighting the problem that critical infrastructure often relies on legacy systems that are less secure and at higher risk. *See* Kovaks, *supra*; Daugherty et al., *supra* note 11, at 13.

65. These claims include breach of contract, negligence, misrepresentation, and deceptive acts and practices. *E.g.*, *In re* Heartland Payment Sys., Inc. Customer Data Sec. Litig., 834 F. Supp. 2d 566 (S.D. Tex. 2011), *rev'd in part sub nom.* Lone Star Nat'l Bank, N. Am. v. Heartland Payment Sys., Inc., 729 F.3d 421 (5th Cir. 2013).

66. *E.g.*, *In re* Target Corp. Customer Data Sec. Breach Litig., 64 F. Supp. 3d 1304, 1309–10 (D. Minn. 2014) (finding that financial institutions that issued credit or debit cards affected by a breach of a retailer's systems adequately pleaded a claim for negligence). Negligence law imposes a duty of reasonable care when a defendant's conduct creates a foreseeable risk of injury. *Id.* at 1308.

67. *Id.* at 1309–10 (applying Minnesota law, which recognizes a duty of reasonable care to protect the security of financial data); *Lone Star Nat'l Bank*, 729 F.3d at 426 (applying New Jersey law); *In re*: The

area of negligence law and not every court recognizes it under its state's common law.[68] Furthermore, what is considered "foreseeable" in data breach litigation is still being defined through case law and regulatory guidance, though it appears to include at least those risks that can be identified through readily available measures[69] or risks that a company knew about but failed to take reasonable security measures to address.[70]

Contractual allocation of the liabilities and costs of responding to a cybersecurity breach in contracts is paramount. Industrial IoT companies often rely on the services of third-party providers, particularly third-party platform or cloud service providers who may store the massive amount of data generated from industrial IoT technologies.[71] If the third party experiences a data breach, the allocation of expenses associated with mitigation, data recovery, customer notification, and potential litigation may depend on the terms of the services contract with the third party.[72] Companies may want to add specific provisions to their contracts assigning responsibility for data breach costs and related litigation expenses, maintaining cybersecurity insurance, setting an appropriate liability cap, or creating a carveout in liability waivers for potential lost profits.[73]

A company may reduce its potential liability for security risks, especially in the face of negligence claims or a regulatory investigation, if it implements appropriate measures up front. There are three approaches a company may consider to reduce potential liability in the event of a cybersecurity incident: implementing (1) risk-based security measures, (2) security by design, or (3) security measures based on industry sector standards and guidelines.

Home Depot, Inc., Customer Data Sec. Breach Litig., No. 2583 1:14-md-2583-TWT, 2016 WL 2897520, at *3–4 (N.D. Ga. May 18, 2016) (applying Georgia law).

68. *See* USAA Fed. Savings Bank v. PLS Fin. Services, Inc., 260 F. Supp. 3d 965, 969–70, 970 n.4 (N.D. Ill. 2017) (refusing to recognize a duty to exercise reasonable care in safeguarding financial information under Illinois law).

69. *See FTC Files Complaint Against LabMD for Failing to Protect Consumers' Privacy*, Fed. Trade Commission (Aug. 29, 2013), https://www.ftc.gov/news-events/press-releases/2013/08/ftc-files-complaint-against-labmd-failing-protect-consumers.

70. *Home Depot*, 2016 WL 2897520, at *4.

71. *See* Nonaka & Rubino, *supra* note 53.

72. *See id.* A company may not receive compensation for these expenses if its contracts with third parties limit or waive indirect, special, exemplary, incidental, or consequential damages or lost profits. *See* Silverpop Sys., Inc. v. Leading Mkt. Tech., Inc., 641 Fed. Appx. 849, 858 (11th Cir. 2016) (holding that a company will not have the right to consequential damages when they are waived in a contract or license agreement). In *Heartland Payment Systems*, banks sued to recover costs they incurred when a company that processed credit card information for the banks experienced a data breach in which hackers stole the credit card information. 834 F. Supp. 2d at 575. The court found that the banks could not recover consequential damages from the payment processor under a breach of contract claim, given that their contract limited this remedy to willful breaches and there was insufficient evidence that the contract breach at issue was willful. *Id.* at 580. Courts do not always agree on what constitutes consequential versus direct damages, so companies should consider negotiating in advance as to which party will be responsible for data breach costs. *See* Colin Quinn & Brendan Quinn, *Awarding Damages for a Breach of Contract: Direct or Consequential?*, J. Kan. B. Ass'n, Oct. 2017, at 21.

73. Nonaka & Rubino, *supra* note 53.

Adopting a risk-based approach to cybersecurity allows a company to demonstrate that it took measures appropriate to the risk faced and reduced potential liability down the road. Some regulators recommend that companies prioritize their security measures based on commonly known or reasonably foreseeable risks,[74] as there is a spectrum of security risks in an industrial environment, and it may be impossible to address all risks lurking in a connected environment.[75] Even attempting to address all risks may result in a frustrating game of cat and mouse, continually responding to new security threats.[76] Instead, a company should conduct an assessment of the risks it actually faces in its industrial environment and tailor its security measures accordingly.[77] Potential risk factors include the size of the company, the number of known risks present in the industrial environment, the criticality of the services the company provides, the size of the potential damage from an attack, the likelihood of an attack occurring, and the economic cost to mitigate an attack.[78] The company should weigh these risk factors against the amount of time, cost, and resources needed to implement security measures to address the threats.[79]

Another approach to reducing potential liabilities is to adopt "security by design" by taking into account security at the outset of designing an industrial IoT system. This would involve companies conducting a risk assessment and incorporating security measures to address those risks before operationalizing equipment with IoT technologies.[80] Some regulators have issued guidance recommending that companies incorporate security by design into the IoT, including the Department of Homeland

74. Many states have data security laws requiring companies handling personal information to develop a comprehensive information security program containing administrative, technical, and physical safeguards appropriate to the size, scope, and type of business, the amount of resources available to the company, the amount of stored data, and the need for security and confidentiality of the information. *See, e.g.*, Cal Civ. Code § 1798.81.5 (West 2018); Md. Code Ann. Com. Law § 14-3503 (West 2018); Or. Rev. Stat. § 646A.622 (2018); 201 Mass. Code Regs. 17.03 (2018). Non-binding federal guidelines similarly recommend the implementation of reasonable administrative, technical, and physical safeguards, particularly to address commonly known or reasonably foreseeable risks. *See generally* Fed. Trade Comm'n, Protecting Personal Information (2015), https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf (providing guidelines to businesses on how to protect their customers' sensitive information).

75. *See* Rose et al., *supra* note 32, at 33 ("In an endless cat-and-mouse game, new security threats evolve, and device manufacturers and network operators continuously respond to address the new threats.").

76. *Id.*

77. *See id.*

78. *See id.*

79. *Id.* At a minimum, a company should aim to adopt any measures that are relatively inexpensive and not disruptive to the business to implement. *See id.* at 33–35 (discussing the importance of security in IoT devices).

80. *See generally* Fed. Trade Comm'n, Internet of Things: Privacy & Security in a Connected World (2015) [hereinafter FTC IoT Guidance], https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf (encouraging companies to "build security into their devices at the outset").

Security,[81] Federal Trade Commission,[82] and National Highway Traffic Safety Administration.[83]

Companies may reduce their exposure to liability by relying on relevant security standards when selecting security measures. In tort law, courts have traditionally examined industry customs or standards to determine best practices, and a company's compliance with those standards may present strong evidence weighing against negligence.[84] The standards set by the National Institute of Standards and Technology (NIST), now part of the U.S. Department of Commerce, apply across industries,[85] and some regulators encourage companies to implement NIST standards.[86] Industry-specific standards are also important to consider.[87]

81. The Department of Homeland Security wants companies to prioritize security in the IoT at the design phase to reduce the risk of disruptions to critical infrastructure and avoid the more difficult and expensive process of adding security to IoT technologies after they have been deployed. U.S. Dept. of Homeland Sec., Strategic Principles for Securing the Internet of Things (IoT) 2, 5 (2016), https://www.dhs.gov/sites/default/files/publications/Strategic_Principles_for_Securing_the_Internet_of_Things-2016-1115-FINAL....pdf.

82. The Federal Trade Commission (FTC) has been a vocal proponent of adopting security by design, urging companies for years not to leave security as an afterthought in developing IoT technologies. FTC IoT Guidance, *supra*, note 80, at 28. Though the FTC gives companies the flexibility to implement context-specific security measures rather than prescribing specific measures, it recommends greater security measures for IoT technologies that collect sensitive information, present physical security or safety risks, or connect to other devices or networks. *Id.* at 33.

83. The National Highway Traffic Safety Administration (NHTSA) encourages vehicle and equipment manufacturers and suppliers to address cybersecurity risks throughout the entire life cycle of the vehicle, including the conception, design, and manufacturing phases, not just the use and maintenance phases, with the goal of designing products free of unreasonable safety risks stemming from cybersecurity threats and vulnerabilities. Nat'l Highway Traffic Safety Admin., Cybersecurity Best Practices for Modern Vehicles 12 (2016) [hereinafter NHTSA Guidance].

84. Michael L. Rustad & Thomas H. Koenig, *The Tort of Negligent Enablement of Cybercrime*, 20 Berkeley Tech. L.J. 1553, 1587–88 (2005).

85. *About NIST*, NIST, https://www.nist.gov/about-nist (last updated June 14, 2017) (explaining NIST's role as a physical science laboratory providing expertise, measurements, and standards for U.S. industries).

86. U.S. Food & Drug Admin., Postmarket Management of Cybersecurity in Medical Devices 14 (2016), https://www.fda.gov/downloads/medicaldevices/deviceregulationandguidance/guidancedocuments/ucm482022.pdf. For example, the FDA recommends that manufacturers seeking approval of medical devices apply the NIST Framework for Improving Critical Infrastructure Cybersecurity ("the Framework") in developing and implementing a cybersecurity program. *Id.* The Framework is a set of standards and best practices developed through a collaboration between the government and the private sector to help organizations manage cybersecurity risks. Nat'l Inst. of Standards & Tech., Framework for Improving Critical Infrastructure Technology 1 (2014), https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf.

87. NHTSA encourages vehicle and equipment manufacturers to implement the SAE J3061 standard, called the Cybersecurity *Guidebook for Cyber-Physical Vehicle Systems*, which vehicle and equipment manufacturers published in January 2016 to recommend best practices and promote a life-cycle approach to address cybersecurity risks in vehicles. NHTSA Guidance, *supra* note 83; *Cybersecurity Guidebook for Cyber-Physical Vehicle Systems J3061*, SAE Int'l (Jan. 17, 2012), http://standards.sae.org/wip/j3061/. SAE International ("SAE") is a professional association of "scientists, engineers, and practitioners that advances self-propelled vehicle and system knowledge" through the development of voluntary consensus standards. *About SAE International*, SAE Int'l, https://www.sae.org/about/ (last visited Apr. 1, 2018).

A company may want to consider whether to participate in the Cybersecurity Information Sharing Act of 2015 (CISA) as part of its cybersecurity defense strategy.[88] CISA permits companies to conduct defensive measures, share cyber threat indicators with the federal government or other companies, and receive information from the federal government about cyber indicators.[89] In return, the company would receive protection from liability for the information it shares with the federal government.[90] However, this liability protection applies only if the company monitors information systems or shares cyber threat indicators in accordance with the procedures provided in CISA.[91] If a company complies in good faith with the reporting procedures but commits a technical violation, it may not benefit from the liability protection.[92] If a company decides to participate in CISA, it should keep careful records documenting its compliance.[93] Furthermore, liability protection appears to apply only to liability arising from the sharing of cyber threat indicators,[94] so a company could still face potential liability for other conduct, such as failing to take reasonable steps to protect against foreseeable risks prior to a data breach. This uncertainty about the scope of liability protections and other legal issues may explain why few companies have chosen to make use of CISA since it was enacted.[95]

III. INTELLECTUAL PROPERTY PROTECTION

Companies have an incentive to seek intellectual property protection for the industrial IoT technologies they develop, given the efficiencies and competitive advantages these technologies may afford them. Intellectual property protection could help companies defend their proprietary technologies and establish legal ownership of early IoT innovations as the IoT space becomes more crowded.[96] Applications for intellectual property protection related to the IoT have risen sharply

88. Cybersecurity Information Sharing Act of 2015, 6 U.S.C. §§ 1501–1510 (2012).

89. 6 U.S.C. §§ 1502–03; U.S. Comp. Emergency Readiness Team, Cybersecurity Information Sharing Act—Frequently Asked Questions (2016), https://www.us-cert.gov/sites/default/files/ais_files/CISA_FAQs.pdf.

90. 6 U.S.C. § 1505 ("No cause of action shall lie or be maintained in any court against any private entity, and such action shall be promptly dismissed . . . .").

91. *Id.*

92. *See* John Evangelakos & Brent J. McIntosh, *A Guide to the Cybersecurity Act of 2015*, Law360 (Jan. 12, 2016, 11:57 AM), https://www.law360.com/articles/745523/a-guide-to-the-cybersecurity-act-of-2015.

93. *Id.*

94. 6 U.S.C. § 1507(k)(1) ("This subchapter supersedes any statute or other provision of law of a State . . . that restricts or otherwise expressly regulates *an activity authorized under this subchapter*." (emphasis added)).

95. *See* Robert Lemos, *Cyber-Threat Data Sharing Off to Slow Start Despite U.S. Legislation*, eWeek (Oct. 2, 2016), http://www.eweek.com/security/cyber-threat-data-sharing-off-to-slow-start-despite-u.s.-legislation.

96. *See* Charles E. Root Jr. & Nancy Edwards Cronin, *The Internet of Things and Intellectual Property: Who Owns the Data?*, ipCapital Group (May 17, 2016, 1:48 PM), http://www.ipcg.com/?file=The_Internet_of_Things_and_Intellectual_Property:_Who_Owns_the_Data.

since 2014.[97] Larger companies in particular have been actively seeking intellectual property protection.[98] Yet it remains unclear the extent to which companies will be able to obtain intellectual property protection, especially patents, for their industrial IoT technologies.[99] IoT technologies consist of the physical hardware, sensors, and devices, as well as more abstract technologies such as software, cloud services, network connectivity, and communications protocols.[100] Recent legal developments may make it harder for companies to obtain intellectual property protection for claims directed to the more abstract technologies.[101]

Software is a critical component of industrial IoT technology, but in 2014, the Supreme Court limited software patent eligibility. In *Alice Corporation v. CLS Bank International*, the Supreme Court held that generic computer implementation of an abstract idea is not sufficient to constitute a patent-eligible invention.[102] A claim directed to an abstract idea generally is excluded from patent eligibility under 35 U.S.C. § 101 and can be patented only if there are additional elements that "transform the nature of the claim into a patent-eligible application."[103] In other words, there must be an "inventive concept."[104]

Post-*Alice*, there is a question of which software claims may be patent-eligible. While *Alice* has reduced patent eligibility for many software claims,[105] courts have deemed some software claims patent-eligible in the last two years.[106] These cases may show promising signs for the patent eligibility of software and computer technology critical to the industrial IoT. In *Enfish, LLC v. Microsoft Corporation*, the

97. Charles E. Root Jr. & Nancy Edwards Cronin, *The Internet of Things (IoT) and Implications for Intellectual Property Part III: Alexa Today, Where Tomorrow?*, ipCapital Group (Jan. 20, 2017, 8:07 PM), http://www.ipcg.com/?file=The_Internet_of_Things_and_Implications_for_Intellectual_Property_Alexa_today_where_tomorrow.

98. Root & Cronin, *supra* note 96.

99. *See infra* notes 102–113 and accompanying text.

100. Charles E. Root Jr. & Nancy Edwards Cronin, *The Internet of Things (IoT) and Implications for Intellectual Property Part One of Three: The Far-Reaching Landscape of IoT*, ipCapital Group (Feb. 18, 2016, 4:07 PM), http://www.ipcg.com/?file=The_Internet_of_Things_Part_One; *IoT Technology Guidebook*, Postscapes, https://www.postscapes.com/internet-of-things-technologies/ (last visited Apr. 2, 2018) (listing examples of IoT technologies).

101. *See infra* notes 102–113 and accompanying text.

102. 134 S. Ct. 2347 (2014) (holding that trading software utilizing third parties to mitigate risk in financial transactions was not patentable, as it merely used a generic computer and generic computer functions to implement the abstract idea of intermediated settlement).

103. *Id*. at 2355 (internal citation and quotation marks omitted) (quoting Mayo Collaborative Servs. v. Prometheus Labs., Inc., 566 U.S. 66, 78 (2012)).

104. *Id*. at 2350. The patents at issue in *Alice* involved a computer-implemented scheme directed to the abstract idea of managing risk in financial transactions, and the Court found that the claims lacked an inventive concept because they merely amounted to a generic computer implementation of recordkeeping. *Id*. at 2352, 2359.

105. Jones Day, Legal Issues Related to the Development of Automated, Autonomous, and Connected Cars 11 (2017) [hereinafter Jones Day White Paper].

106. *See infra* notes 107–113 and accompanying text.

Federal Circuit concluded that "claims directed to improvements in computer-related technology, including those directed to software," are not necessarily abstract and may be patent-eligible.[107] When a patent claim is "directed to an improvement to computer functionality," rather than merely using a computer as a tool, the claim is not abstract and therefore is patent-eligible.[108] The technology at issue in *Enfish* was a self-referential computer database that improved the efficiency and flexibility of information storage.[109] While the district court found that the claimed idea was simply directed at the abstract idea of storing and organizing information, the Federal Circuit reversed that decision because the self-referential table *improved* the functionality of information storage by storing information "related to each column in rows of that very same table, such that new columns can be added by creating new rows in the table."[110]

Even for abstract ideas, all may not be lost post-*Alice*. A company may still be able to demonstrate that an abstract idea contains an inventive concept, and thus is patent-eligible, where the patent claim provides for a specific and discrete way to implement the abstract idea. In *Bascom Global Internet Services, Inc. v. AT&T Mobility LLC*, the patent claim was a filtering software at the ISP server level that allowed subscribers to control websites accessed and information received over the internet; the software improved on existing filtering tools by allowing the filters to be customized for each individual user rather than having a universal set of filtering rules.[111] While filtering software is directed to an abstract idea, the Federal Circuit nevertheless concluded that the filtering software in *Bascom* was patent-eligible because it contained an inventive concept.[112] The inventive concept was "the installation of a filtering tool at a specific location, remote from the end-users, with customizable filtering features specific to each end user. This design gives the filtering tool both the benefits of a filter on a local computer and the benefits of a filter on the ISP server."[113]

While it is not clear post-*Alice* the extent to which companies could obtain a patent for data analysis software critical to the industrial IoT,[114] these cases demonstrate a potential path forward. Software developed for the industrial IoT is

107. 822 F.3d 1327, 1335 (Fed. Cir. 2016). The U.S. Patent and Trademark Office periodically provides updated guidance on identifying abstract ideas. *Subject Matter Eligibility*, U.S. Pat. & Trademark Off., https://www.uspto.gov/patent/laws-and-regulations/examination-policy/subject-matter-eligibility (last visited Apr. 1, 2018).

108. *Enfish*, 822 F.3d at 1335–36.

109. *Id.* at 1333.

110. *Id.* at 1337–38.

111. 827 F.3d 1341, 1343–44 (Fed. Cir. 2016).

112. *Id.* at 1350.

113. *Id.* This "specific method of filtering [i]nternet content cannot be said . . . to have been conventional or generic," and "its particular arrangement of elements is a technical improvement over prior art ways of filtering such content." *Id.*

114. *See* W. Keith Robinson, *Patent Law Challenges for the Internet of Things*, 15 Wake Forest J. Bus. & Intell. Prop. L. 655, 667 (2015).

generally designed to improve the computing process by enabling machines to interact with the physical world and store and analyze that information in new ways. To the extent such software improves computer functionality or advances a technology, a claim could possibly fit within *Enfish*'s analysis of patent eligibility. If a software claim is deemed an abstract idea, it may nevertheless be patent-eligible along the lines of the *Bascom* analysis if the claim provides a specific method for analyzing, storing, or organizing data from the physical world.

IV. INTEROPERABILITY AND LICENSING

The interoperability of technology is necessary to fulfill the industrial IoT's promise of a network of sensors and transmitters that communicate and process information seamlessly.[115] In the past, large industrial companies have built their own industrial IoT platforms using technologies designed to integrate throughout the industrial system.[116] Recently we are seeing more players developing varied industrial IoT technologies.[117] In 2016, there was more than $2.2 billion invested in startups that focus on industrial digitization by developing sensors, cloud platforms, networking infrastructure, and machine-learning software.[118] Yet having so many proprietary products may hinder interoperability across models or manufacturers. It is estimated that forty percent of the IoT's potential value depends on interoperability,[119] but to create interoperability there must be standardized technology to connect objects and process information from varying sources. Until a degree of standardization is achieved, the full potential of these technologies may not be realized.

A challenge to standardization is the potential for an industrial company to risk infringing third party patents or pay high licensing fees.[120] Given the large number of code and technologies needed to operate the IoT at an industrial level,[121] it would be easy to infringe a third-party patent. One way to address this challenge is by creating standard essential patents (SEPs) that require a patent holder to offer non-exclusive licenses on fair, reasonable, and non-discriminatory (FRAND) terms.[122] SEPs are patents of core technologies that are essential to comply with an industry standard.[123] This solution has been used in other industries, most notably the

115. *See* Paez & La Marca, *supra* note 1, at 34.

116. *See* CB Insights, *supra* note 12.

117. *Id.*

118. *Id.*

119. Manyika et al., *supra* note 14, at 23.

120. *See* Paez & La Marca, *supra* note 1, at 35.

121. *E.g.*, Shackelford & Russell, *supra* note 31.

122. *See* Robin Kester, Note, *Demystifying the Internet of Things: Industry Impacts, Standardization Problems, and Legal Considerations*, 8 Elon L. Rev. 205, 223 (2016).

123. EC Roadmap, *supra* note 21, at 1.

smartphone industry,[124] and has been gaining traction as a potential solution in the IoT area.[125]

However, it is not clear that using FRAND terms to set licensing deals will be as successful in the IoT area as it was in the mobile phone industry.[126] First, a set of standards would need to be developed in the IoT space.[127] This would not be an easy task as the standards would need to apply to a wide range of technologies, and there may be uncoordinated or conflicting strategies among industry coalitions and even across countries.[128] Second, it may be difficult to identify core technologies and determine which patents are essential.[129] In the IoT area, a large number of sensors and technologies are needed to operate the IoT at an industrial level,[130] which makes identifying those central to a standard more difficult.[131] Third, stakeholders may not agree on what is a fair and reasonable licensing fee.[132] Making the task more difficult still is that there are no widely agreed upon valuation methodologies, and using different methodologies would harm the predictability of licensing fees.[133]

Another potential solution to the risk of infringement or high licensing fees is the creation of patent pools. A patent pool occurs when companies that hold patents to different components of a particular technology pool their patents and work as one group to license the technology as a whole.[134] The benefit is that if another company wants to license that technology, it has to negotiate with only the single group, rather than with each of the entities individually, to set the licensing terms.[135] However, the IoT has a wider "range of industrial stakeholders," and a large number of sensors and

124. Paez & La Marca, *supra* note 1, at 36; *A Note on Standard Essential Patents*, Clairvolex (Jan. 2017), https://clairvolex.com/PDFs/January-2017-Mailer.pdf ("Almost all smartphones or tablets that we use today are protected by one or more SEPs.").

125. Recently, the European Commission announced its goal to promote the interoperability of IoT through FRAND to further digital integration within the European Union and maintain global competitiveness. EC Roadmap, *supra* note 21.

126. *See* Paez & La Marca, *supra* note 1, at 36–37.

127. Rose et al., *supra* note 32, at 7.

128. *Id.* at 47–49.

129. EC Roadmap, *supra* note 21, at 2.

130. *E.g.*, Shackelford & Russell, *supra* note 31.

131. *See* EC Roadmap, *supra* note 21, at 2; Patricia Cappyuns & Jozefien Vanherpe, *The Scoop from Europe: Europe Takes on FRAND Licensing—Again*, 52 les Nouvelles 122, 124–26 (2017).

132. *See* Cappyuns & Vanherpe, *supra* note 131, at 122, 124–26.

133. EC Roadmap, *supra* note 21, at 2. Recognizing the importance of valuation methodologies, the European Commission has issued a roadmap outlining a forthcoming initiative to provide guidance on FRAND and valuation principles. *Id.* at 3.

134. Freek Vermeulen, *Patent Pools: Do They Kill Innovation?*, Forbes (Jan. 22, 2013, 4:39 PM), https://www.forbes.com/sites/freekvermeulen/2013/01/22/patent-pools-do-they-kill-innovation/#d1cdabb58f4d.

135. *See id.*

technologies are needed to operate the IoT at an industrial level.[136] It is not clear that the diverse range of stakeholders, with their own set of interests, customers, and revenue goals, will be able to work together on licensing deals.[137]

Some degree of standardization may be achieved as more companies rely on open source technology, which saves those companies valuable time and resources.[138] However, use of open source software often requires a license, and the license may be difficult to administer.[139] Users of open source software licenses must provide notice of their use of the software in accordance with procedures, seek approval to use the software, and provide assurance that they will comply with the licenses.[140] A company that fails to comply with open source software licenses may be subject to a copyright infringement or breach of contract lawsuit.[141]

Interoperability is important to the success of the industrial IoT, but there is no simple way to achieve it without risking potential legal exposure. It could take years for standard-setting bodies to develop appropriate standards, but waiting for coordination of these dispersed efforts could delay the benefits of the industrial IoT. Industrial companies could face potential patent infringement claims, licensing risk, and intellectual property litigation as they navigate the fragmented industrial IoT environment.

V. RISKS AND LIABILITIES BY SECTOR

Certain industries have been early adopters of the industrial IoT and are leading investment in the technologies and software necessary to implement it.[142] The transportation, health care, and utilities sectors are among those early adopters.[143]

136. Wireless Watch, *Ericsson's Patent Pool is Far from the New Start the IoT Needs*, Register (Oct. 3, 2016, 8:02 AM), https://www.theregister.co.uk/2016/10/03/ericssons_patent_pool_is_far_from_the_new_start_the_iot_needs/.

137. *Id.* Some commentators have criticized patent pools for harming innovation; if the pool decides to include a component by one company, but not a close substitute by another company, there may be decline in innovation among companies that exist outside the pool. Vermeulen, *supra* note 134.

138. Naomi Tajitsu, *Toyota Uses Open-Source Software in New Appproach to In-Car Tech*, Reuters (May 31, 2017, 7:00 AM), http://www.reuters.com/article/us-toyota-tech-idUSKBN18R1CW. In the automotive industry, Automotive Grade Linux is a collaborative open source platform for connected cars currently being developed jointly by ten automakers. *Id.*; *see also* The Linux Found., *About*, Automotive Grade Linux, https://www.automotivelinux.org/ (last visited Apr. 1, 2018). A connected car may use over one hundred million lines of code, and relying on open source code saves an automaker from engaging in the time-consuming process of coding from the ground up for each car model and enables the company to focus on customizing applications. Tajitsu, *supra*.

139. Jones Day White Paper, *supra* note 105, at 13.

140. *Id.*

141. *Id.*; *e.g.*, Artifex Software, Inc. v. Hansom, Inc., No. 16-cv-06982-JSC, 2017 U.S. Dist. LEXIS 62815 (N.D. Cal. Apr. 25, 2017) (upholding a breach of contract claim alleging breach of an open source software agreement).

142. Alison DeNisco Rayome, *The Five Industries Leading the IoT Revolution*, ZDNet (Feb. 1, 2017, 11:36 AM), http://www.zdnet.com/article/the-five-industries-leading-the-iot-revolution/.

143. *Id.*

These industries provide insight into the legal risks and liabilities likely to come as more companies incorporate the industrial IoT into their operations.

A. Transportation

Industrial IoT technologies have the capability to significantly transform the way people travel and to improve public safety,[144] but they present manufacturers, suppliers, and operators with new legal issues, regulatory challenges, and potential liabilities that are only just starting to be addressed. IoT technologies can apply to all forms of transportation and traffic infrastructure, though connected vehicles and airplanes are among the more advanced IoT applications in the transportation sector.[145] A "connected" vehicle or airplane can access the internet, often through a wireless network, and communicate with the physical environment, infrastructure, and manufacturers.[146] These connected features allow the vehicles and airplanes to send and receive streams of data through the internet for the purpose of monitoring wear and tear of parts, navigation, collision avoidance, weather and traffic reports, entertainment, and emergency notifications.[147]

A pressing concern for companies is managing the cybersecurity risks associated with connected transportation technology. The advanced wireless features that make connected transportation technologies possible also present serious safety risks if they malfunction or are accessed by hackers. Researchers have demonstrated it is possible for hackers to obtain functional control over the operation of a vehicle or airplane through connected technologies.[148]

---

144. Franklin Morris, *Five Ways IoT Will Change How You Experience Air Travel*, IBM: Internet of Things Blog (Oct. 13, 2016), https://www.ibm.com/blogs/internet-of-things/smart-air-travel/ ("Thanks to IoT devices and analytics, [we are] poised to see the airline industry move toward greater efficiency and better customer service.").

145. Andrew Meola, *How the Internet of Things Will Transform Private and Public Transportation*, Bus. Insider (Dec. 21, 2016, 11:11 AM), http://www.businessinsider.com/internet-of-things-connected-transportation-2016-10.

146. Jones Day White Paper, *supra* note 105, at 2.

147. Christine Hall, *BMW's Connected-Car Data Platform to Run in IBM's Cloud*, Data Ctr. Knowledge (June 16, 2017), http://www.datacenterknowledge.com/archives/2017/06/16/bmws-connected-car-data-platform-to-run-in-ibms-cloud/; Gillian Jenner, *How Airlines Are Tapping into the Internet of Things*, Gen. Electric, https://www.ge.com/digital/press-releases/how-airlines-are-tapping-internet-things (last visited Apr. 1, 2018).

148. Researchers have demonstrated the ability to remotely shut down engines, disable brakes, control steering, lock doors, and use turn signals in connected vehicles, or change the position of airplanes. *Public Service Announcement: Motor Vehicles Increasingly Vulnerable to Remote Exploits*, Fed. Bureau Investigation (Mar. 17, 2016), https://www.ic3.gov/media/2016/160317.aspx; Kim Zetter, *Feds Say that Banned Researcher Commandeered a Plane*, Wired (May 15, 2015, 10:14 PM), https://www.wired.com/2015/05/feds-say-banned-researcher-commandeered-plane/ [hereinafter *Researcher Commandeered a Plane*]; *see also* Chris Valasek & Charlie Miller, IOActive, Remote Exploitation of an Unaltered Passenger Vehicle (2015), https://www.ioactive.com/pdfs/IOActive_Remote_Car_Hacking.pdf (detailing research on the vulnerability of connected automobiles). For example, white hat hackers conducted a test where they hacked a Jeep Cherokee driving seventy miles per hour in downtown St. Louis, Missouri and cut the transmission so that the test driver could not accelerate by pressing the

Federal policy addressing transportation cybersecurity has developed in a piecemeal fashion, though momentum is building toward improving cybersecurity efforts. In January 2017, the National Highway Traffic Safety Administration (NHTSA) issued a Notice of Proposed Rulemaking requiring vehicle-to-vehicle (V2V) technology[149] in all cars and light trucks.[150] To address security concerns, the proposal would require "firewalls" between V2V modules and other modules connected to the data system[151] and allow for periodic software updates.[152] NHTSA released its latest policy in September 2017 containing Voluntary Guidance for Automated Driving Systems outlining twelve safety principles, including a recommendation to minimize safety risks from hacking by following industry best practices.[153] The Federal Aviation Administration (FAA) has begun efforts to address cybersecurity,[154] though the General Accountability Office issued a report to members of Congress stating that the FAA should develop a more comprehensive approach to cybersecurity as it transitions to the Next Generation Air Transportation

gas pedal. Andy Greenberg, *Hackers Remotely Kill a Jeep on the Highway—With Me in It*, Wired (July 21, 2015, 6:00 AM), https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/. A "white hat" hacker generally refers to security researchers or other hackers who notify a vendor or other responsible party when they discover a software vulnerability. Kim Zetter, *Hacker Lexicon: What Are White Hat, Gray Hat, and Black Hat Hackers?*, Wired (Apr. 13, 2016, 5:03 PM), https://www.wired.com/2016/04/hacker-lexicon-white-hat-gray-hat-black-hat-hackers/. Similarly, a researcher claimed that he was able to take control of an airplane after hacking the in-flight entertainment system and caused the engines to climb, resulting in a sideways movement of the plane during flight. *Researcher Commandeered a Plane*, *supra*.

149. With V2V technology, "[c]ars will talk to other cars, exchanging data and alerting drivers to potential collisions. They'll talk to sensors on signs on stoplights, bus stops, even ones embedded in the roads to get traffic updates and rerouting alerts. And they'll communicate with your house, office, and smart devices." Dirk Wollschlaeger, *What's Next? V2V (Vehicle-to-Vehicle) Communication with Connected Cars*, Wired, https://www.wired.com/insights/2014/09/connected-cars/ (last visited Apr. 1, 2018).

150. Federal Motor Vehicle Safety Standards; V2V Communications, 82 Fed. Reg. 3854, 3855 (proposed Jan. 12, 2017) (to be codified at 49 C.F.R. pt. 571). The proposal contained V2V communications performance requirements tied to the dedicated short-range communication (DSRC) protocol, which is a two way short- to medium-range wireless communications capability that permits high data transmission critical to safety applications. *DSRC: The Future of Safer Driving*, U.S. Dep't Transp., https://www.its.dot.gov/factsheets/dsrc_factsheet.htm (last visited Apr. 1, 2018). The proposal is facing resistance from those who believe that 5G networks can better handle V2V communications. John R. Quain, *Cars Will Talk to One Another. Exactly How Is Less Certain.*, N.Y. Times (Mar. 9, 2017), https://www.nytimes.com/2017/03/09/business/cars-v2v-dsrc-communication.html.

151. These "firewalls" are proposed "to help isolate V2V modules [from] being used as a potential conduit into other vehicle systems." Federal Motor Vehicle Safety Standards; V2V Communications, 82 Fed. Reg. at 3856–57.

152. *Id.* at 3856, 3914–15.

153. Jones Day White Paper, *supra* note 105, at 6.

154. Aliya Sternstein, *FAA Working on New Guidelines for Hack-Proof Planes*, Nextgov (Mar. 4, 2016), http://www.nextgov.com/cybersecurity/2016/03/faa-has-started-shaping-cybersecurity-regulations/126449/; Andy Pasztor, *FAA Advisory Body Recommends Cybersecurity Measures*, Wall Street J., https://www.wsj.com/articles/faa-advisory-body-recommends-cybersecurity-measures-1474587049 (last updated Sept. 22, 2016, 9:47 PM).

System, which relies more heavily on integrated information systems and digital communication methods.[155]

Use of connected technologies generates intellectual property concerns. Automated or connected vehicles will require the development of key technologies, including collision avoidance technologies, digital cameras, Light Detection and Ranging (LiDAR),[156] radar, telecommunications (including DSRC and 5G capabilities), artificial intelligence, machine learning, sensors, and mesh networking technology.[157] Companies developing these technologies need to protect their intellectual property rights through trade secrets or patents.[158]

Although thousands of patents have already been issued to original equipment manufacturers, suppliers, and technology companies for connected transportation technology,[159] as noted earlier, the Supreme Court's decision in *Alice* has thrown into question the extent to which these patents will be issued given that industrial IoT technologies are increasingly software-related.[160] For example, in 2015, the Federal Circuit found a patent to screen equipment and vehicle operators for impairment invalid because the patent's application lacked details specifying how the screening system worked or improved results over prior art, and lacked an inventive concept beyond conventional computer implementation.[161] Going forward, companies seeking patents for transportation technologies should be careful to show how the invention improves the operation of a computer or advances a technology.[162]

Alternatively, companies may seek to protect their technologies through trade secret law.[163] The benefits of relying on trade secret law to protect IoT technologies are that trade secret protection is relatively inexpensive to obtain, it can be established faster than prosecution of a patent application, it contains no subject matter limitation,

155. U.S. Gov't Accountability Office, GAO-15-370, Air Traffic Control: FAA Needs a More Comprehensive Approach to Address Cybersecurity as Agency Transitions to NextGen 1, 11 (2015), https://www.gao.gov/assets/670/669627.pdf.

156. LiDAR is a remote sensing method used to examine the surface of the Earth. *What is LIDAR?*, Nat'l Oceanic & Atmospheric Admin., https://oceanservice.noaa.gov/facts/lidar.html (last updated Oct. 10, 2017).

157. Jones Day White Paper, *supra* note 105, at 10.

158. *Id.*

159. *Id.*

160. *See id.* at 11.

161. *Vehicle Intelligence & Safety LLC v. Mercedes–Benz USA, LLC*, 635 Fed. Appx. 914, 916, 919–20 (Fed. Cir. 2015).

162. Jones Day White Paper, *supra* note 105.

163. An example is the recently settled lawsuit in which Waymo LLC accused Uber Technologies, Inc. and other defendants of stealing trade secrets related to LiDAR by hiring a senior Waymo engineer who downloaded thousands of confidential company documents. *Waymo LLC v. Uber Technologies, Inc.*, No. 17-cv-00939-WHA, 2017 WL 3581171, at *1 (N.D. Cal Aug. 18, 2017); Jones Day White Paper, *supra* note 105, at 12; Daisuke Wakabayashi, *Uber and Waymo Settle Trade Secrets Suit Over Driverless Cars*, N.Y. Times (Feb. 8, 2018), https://www.nytimes.com/2018/02/09/technology/uber-waymo-lawsuit-driverless.html.

and can be defined during the course of litigation.[164] But trade secrets lack the presumed validity of a patent, protections can vary by state law, disclosure prevents a company from obtaining a legal remedy, and providers of funding tend to prefer patents.[165]

Finally, connected technologies in the transportation sector present potential litigation risk. Manufacturers could be subject to product liability litigation for defective product claims in the event of an accident.[166] Though there have been few product liability claims, one closely watched accident involved a Tesla Model S owner who was killed using the Autopilot feature when his car crashed into a tractor-trailer that crossed the road in front of the car.[167] The accident presented product liability concerns because the automatic emergency braking system did not provide a warning, though NHTSA's initial investigation did not find any defects in the "Autopilot" or braking systems.[168] However, the National Transportation Safety Board issued a new finding on September 12, 2017 indicating that the crash may have been caused by the truck driver's failure to yield and the Tesla driver's inattention due to overreliance on vehicle automation.[169] This finding raises the issue of negligence and the extent to which a human driver can be held liable for inattentiveness when operating an automated vehicle.[170] It also illustrates how potential future litigation may require the allocation of responsibility among the manufacturer, supplier, or operator, some of which may be addressed in advance with a contract and insurance scheme.[171]

B. Health Care

The health care industry is undergoing a digital transformation. Use of IoT technologies improves medical outcomes for individual patients, and, combined with artificial intelligence and big data, the information generated by connected technologies can be used to develop new treatments and predict health care trends

---

164. Jones Day White Paper, *supra* note 105, at 12; Shackelford & Russell, *supra* note 31, at 643.

165. *See* Jones Day White Paper, *supra* note 105, at 12.

166. *Id.* at 15–16.

167. Nat'l Highway Traffic Safety Admin., U.S. Dept. of Transp., PE 16-007, ODI Resume 1 (2017) [hereinafter NHTSA Tesla Report], https://static.nhtsa.gov/odi/inv/2016/INCLA-PE16007-7876.PDF; Darrell Etherington, *NHTSA's Full Final Investigation into Tesla's Autopilot Shows 40% Crash Rate Reduction*, TechCrunch (Jan. 19, 2017), https://techcrunch.com/2017/01/19/nhtsas-full-final-investigation-into-teslas-autopilot-shows-40-crash-rate-reduction/.

168. *See* NHTSA Tesla Report, *supra* note 167, at 1.

169. *Driver Errors, Overreliance on Automation, Lack of Safeguards, Led to Fatal Tesla Crash*, Nat'l Transp. Safety Board, (Sep. 12, 2017), https://www.ntsb.gov/news/press-releases/Pages/PR20170912.aspx. Another accident, in March 2018, involved an Uber self-driving vehicle that hit and killed a pedestrian in Arizona; NHTSA is still investigating the incident and has not determined fault, though there are early indications that neither the driver nor the vehicle detected the individual. Daisuke Wakabayashi, *Uber Ordered to Take Its Self-Driving Cars Off Arizona Roads*, N.Y. Times (Mar. 16, 2018), https://www.nytimes.com/2018/03/26/technology/arizona-uber-cars.html.

170. *See* Jones Day White Paper, *supra* note 105, at 16–17.

171. *See id.* at 16–18.

across the larger population.[172] Smart monitoring devices can assess medical conditions like diabetes, cholesterol levels, or heart disease in real time and automate the delivery of medicine to a patient.[173] Given that these smart devices can collect millions of pieces of information from individuals, IoT technologies can revolutionize health care by delivering that information to medical providers and researchers, who can analyze the data collectively to identify trends and determine where resources can be most effectively allocated.[174]

Health care companies are particularly vulnerable to cybersecurity risks because they collect, store, and maintain a treasure trove of data. These companies handle not only the most sensitive types of personal information, such as social security, credit card, and bank account numbers, but also health care data, which, once disclosed, cannot be changed or canceled like a credit card or bank account number.[175] The health care industry experienced more data breaches than any other critical infrastructure sector in 2015.[176]

Congress established the Health Care Industry Cybersecurity Task Force in the Cybersecurity Act of 2015 to review the cybersecurity challenges facing the health care industry.[177] The Task Force issued its report and recommendations in June 2017.[178] Among the Task Force's chief concerns is the regulatory compliance risk faced by companies in the health care industry.[179] The Task Force noted that multiple regulators have authority within the health care space: The Department of Health and Human Services (HHS), the Office of Civil Rights (OCR) at HHS, the Food and Drug Administration (FDA), and the Office of the National Coordinator for Health

172. Daniel Newman, *Top Five Digital Transformation Trends in Health Care*, Forbes (Mar. 7, 2017, 8:14 AM), https://www.forbes.com/sites/danielnewman/2017/03/07/top-five-digital-transformation-trends-in-healthcare/#6157a75c2561.

173. Geoff Appelboom et al., Smart Wearable Body Sensors for Patient Self-Assessment and Monitoring 3–4 (2014), https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4166023/pdf/2049-3258-72-28.pdf; *see* Health Care Indus. Cybersecurity Task Force, U.S. Dep't Health & Human Servs., Report on Improving Cybersecurity in the Health Care Industry 14 (2017), https://www.phe.gov/Preparedness/planning/CyberTF/Documents/report2017.pdf.

174. *See* Newman, *supra* note 172. For example, one company collects radiological data from millions of x-ray, magnetic resonance imaging (MRI), and tomography readings taken through advanced imaging equipment to analyze how radiologists are using the equipment and make recommendations on how to deploy this expensive equipment more efficiently. Daugherty et al., *supra* note 11.

175. Health Care Indus. Cybersecurity Task Force, *supra* note 173. For this reason, health care data can fetch a higher price for cybercriminals on the dark web. *Id.* at 15.

176. *Id.* at 16. The attacks increased in sophistication in 2016 and 2017 with a wave of ransomware attacks on hospitals and other health-care related organizations. *Id.*; Elizabeth Snell, *Healthcare Ransomware Attacks Contribute to 2017 Top Data Breaches*, HealthITSecurity (Dec. 13, 2017), https://healthitsecurity.com/news/healthcare-ransomware-attacks-contribute-to-2017-top-data-breaches.

177. Health Care Indus. Cybersecurity Task Force, *supra* note 173, at 1.

178. *Id.* at iii.

179. *Id.* at 11–12.

Information Technology at HHS, among others.[180] This may create overlapping and possibly conflicting legal and technical burdens on health care companies.[181]

Privacy and security of health data are regulated generally by the Health Insurance Portability and Accountability Act (HIPAA), as amended by the Health Information Technology for Economic and Clinical Health Act, which protects the storage, handling, and transmission of individuals' protected health information (PHI).[182] HIPAA's Privacy Rule governs the permissible use and disclosure of PHI and grants individuals certain rights to access and correct their healthcare records,[183] while the Security Rule requires entities to safeguard electronic PHI with appropriate policies and procedures to protect PHI from unauthorized access or disclosure.[184] The OCR has an active enforcement history of imposing corrective measures or a civil monetary penalty, or both, on companies that do not fulfill their obligations under these rules.[185] But HIPAA only applies to "covered entities," typically, health care providers, health plans, and health care clearinghouses,[186] and their contractors, called business associates.[187] Certain entities in the industrial IoT space may not be subject to HIPAA, such as suppliers or equipment manufacturers,[188] creating different regulatory burdens for different IoT companies in the health care space.

Companies also face compliance risk with the FDA, which has incorporated cybersecurity recommendations for medical devices into a series of guidance issued over the last few years. Medical devices present some of the greatest cybersecurity risks because they hold a large amount of sensitive patient health information and interact physically with the patient, creating potential for injury to the patient if the device malfunctions. On October 2, 2014, the FDA released guidance called "Content of Premarket Submissions for Management of Cybersecurity in Medical Devices" advising medical device manufacturers to develop a set of cybersecurity controls to

180. *Id.* at 11.

181. *Id.* at 11–12.

182. Health Insurance Portability and Accountability Act, Pub. L. No. 104-191, 110 Stat. 1936 (codified as amended in scattered sections of 18, 29, and 42 U.S.C.), *amended by* Health Information Technology for Economic and Clinical Health Act, Pub. L. No. 111-5, 123 Stat. 115, 230 (codified as amended in scattered sections of 42 U.S.C.).

183. HIPAA Privacy Rules, 45 C.F.R. §§ 164.500–164.534 (2018).

184. HIPAA Security Rules, 45 C.F.R. §§ 164.302–164.318 (2018).

185. *See Enforcement Highlights*, U.S. Dep't Health & Hum. Services, https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/data/enforcement-highlights/index.html?language=en (last updated Mar. 6, 2018).

186. 45 C.F.R. § 160.103 (2018).

187. *Id.* A "business associate" is generally someone who "creates, receives, maintains, or transmits protected health information for a [regulated] function or activity . . . [o]n behalf of such covered entity or of an organized health care arrangement." *Id.*

188. *See* Health Care Indus. Cybersecurity Task Force, *supra* note 173, at 12.

ensure functionality and safety of the devices.[189] The guidance recommends that manufacturers incorporate cybersecurity safeguards during the design and development of the medical device, taking into account the need to balance cybersecurity with the usability of the device.[190]

The FDA also issued guidance on September 6, 2017 called "Design Considerations and Pre-market Submission Recommendations for Interoperable Medical Devices" addressing the cybersecurity of interoperable medical devices.[191] The FDA issued the guidance because "electronic medical devices are increasingly connected to each other and to other technology, [and] the ability of these connected systems to safely and effectively exchange and use the information that has been exchanged becomes increasingly important."[192] The FDA recognized that errors or interference with interoperability could cause inaccurate, untimely, or misleading information that could lead to patient injury or possibly death, such as if a device was to transmit the wrong amount of medicine to a patient.[193] The FDA recommends that manufacturers perform a risk analysis and testing to determine the risks associated with interoperability to the device, the network, and other interfaced devices so that they may implement appropriate security features.[194]

In addition, the Medical Device Cybersecurity Act of 2017 was introduced in the Senate in July 2017 to protect patient safety by proposing a cyber report card for devices, requiring cybersecurity risk assessments, mandating product testing prior to sale, and improving remote access protection for devices, among other measures.[195] Though no action has been taken on the bill yet, it has received support from the health care industry.[196]

---

189. Ctr. For Devices & Radiological Health & Ctr. for Biologics Evaluation & Research, U.S. Food & Drug Admin., Content of Premarket Submissions for Management of Cybersecurity in Medical Devices 3 (2014), https://www.fda.gov/downloads/medicaldevices/deviceregulationandguidance/guidancedocuments/ucm356190.pdf.

190. *Id.* at 4. In particular, manufacturers should consider implementing features such as authentication of users, automatic timed methods to terminate sessions, secure data transfer mechanisms, features to detect security compromises, and features to protect critical functionality of the device in the event of a cybersecurity compromise. *Id.* at 5.

191. Ctr. for Devices & Radiological Health & Ctr. for Biologics Evaluation & Research, U.S. Food & Drug Admin., Design Considerations and Pre-Market Submission Recommendations for Interoperable Medical Devices 1 (2017), https://www.fda.gov/downloads/medicaldevices/deviceregulationandguidance/guidancedocuments/ucm482649.pdf.

192. *Id.*

193. *Id.* at 3.

194. *Id.* at 8.

195. S. 1656, 115th Cong. (2017).

196. Elizabeth Snell, *Medical Device Cybersecurity Act Draws Industry Support*, HealthITSecurity.com (Aug. 4, 2017), https://healthitsecurity.com/news/medical-device-cybersecurity-act-draws-industry-support.

In light of this potential legislation and the regulatory push from the FDA, manufacturers should improve the cybersecurity of their medical devices proactively.[197] For example, manufacturers are already permitted to update the cybersecurity of medical devices without FDA review or approval.[198] Companies that incorporate off-the-shelf software in their medical devices are responsible for ensuring the security and the effective performance of those devices, so companies should test the functionality of their software and update as needed.[199]

Contracting risk is another challenge facing industrial IoT companies in the health care industry. Health care companies making use of the industrial IoT rely on cloud services for data storage, industrial health software solutions, and computing services.[200] In recognition of the widespread use of cloud computing solutions in the healthcare space, HHS issued guidance in October 2016 clarifying that a cloud service provider is a business associate under HIPAA and that a covered entity must enter into a business associate agreement with a cloud service provider involved in creating, receiving, maintaining, or transmitting electronic PHI that complies with the Security Rule.[201] A cloud service provider must comply with these requirements even if it stores encrypted data and does not have the decryption key.[202] HHS also recommends a service level agreement with the cloud service provider to specify business expectations pertinent to HIPAA compliance, such as system availability, data backup and recovery, the manner in which data will be provided to the covered entity upon termination of the agreement, a delineation of responsibility for security, and limits on data retention and disclosure.[203]

These contracting guidelines have implications for cloud service providers who may not even be aware they are handling health care information.[204] The guidelines apply to cloud service providers that do not have actual or constructive knowledge that a covered entity or business associate is using its services to create, receive, maintain, or transmit electronic PHI.[205] HIPAA provides these services providers

197. *FDA Fact Sheet: The FDA's Role in Medical Device Cybersecurity*, U.S. Food & Drug Admin., https://www.fda.gov/downloads/MedicalDevices/DigitalHealth/UCM544684.pdf (last visited Apr. 2, 2018).

198. *Id.*

199. *See id.*

200. *See infra* notes 201.

201. *Guidance on HIPAA & Cloud Computing*, U.S. Dep't Health & Hum. Services, https://www.hhs.gov/hipaa/for-professionals/special-topics/cloud-computing/index.html (last updated June 16, 2017). The agreement should establish the permitted uses and disclosures of electronic PHI and require the business associate to implement appropriate safeguards for electronic PHI, report to the covered entity any unauthorized use or disclosure of electronic PHI, make available its internal practices, books, and records related to the use or disclosure of electronic PHI, and destroy or return to the covered entity all PHI at the termination of the contract, among other requirements. 45 C.F.R. § 164.504(e)(2) (2018).

202. *Guidance on HIPAA & Cloud Computing*, *supra* note 201.

203. *Id.*

204. *Id.*

205. *Id.*

with an affirmative defense, as long as the provider corrects its non-compliance with HIPAA within thirty days.[206]

C. Utilities

One of the most sensitive applications of the industrial IoT is in utilities. Utilities such as power grids, water treatment plants, chemical facilities, and nuclear plants are critical infrastructure that manage the physical world, so interference with IoT technologies at these locations could place public health and safety at risk.[207] Despite the risks, industrial IoT technologies have great potential to modernize utilities that are running inefficiently and operating at capacity with aging legacy equipment, and may not otherwise meet future needs.[208] The application of IoT to utilities will even benefit municipalities in developing smart cities.[209]

Utilities face challenges as they incorporate new technologies. For example, electric utilities operate across a grid—a network of transmission lines, substations, and transformers that delivers electricity from a power plant to customers.[210] The "smart grid" refers to the two-way communication between a utility and customers using controls, automation, digital technologies, and IoT technologies to ensure more efficient transmission of electricity at a lower cost.[211] As utilities continue transitioning toward more digitalization and interconnected networks, the security risks facing these utilities will continue to grow.[212]

A utility is more likely to face enforcement risk than litigation risk arising out of a security incident. Historically, customers or other end users have found it difficult to state a claim for negligence related to interrupted services.[213] Courts have found

206. *Id*.

207. Manyika et al., *supra* note 14, at 105; *see, e.g.*, Zetter, *supra* note 29.

208. Christopher Bosch, Note, *Securing the Smart Grid: Protecting National Security and Privacy Through Mandatory, Enforceable Interoperability Standards*, 41 Fordham Urb. L. J. 1349, 1351 (2014); U.S. Dep't of Energy, *What Is the Smart Grid?*, Smartgrid.gov, https://www.smartgrid.gov/the_smart_grid/smart_grid.html (last visited Apr. 1, 2018).

209. *See Intelligent Urban Water Supply Testbed*, Indus. Internet Consortium, http://www.iiconsortium.org/intelligent-urban-water-supply.htm (last visited Apr. 1, 2018). Municipalities can apply connected technologies to water supply assets, such as pressurizing pumps or water meters, to gather data about water usage, quality, and leakage to ensure equitable water distribution and consumption during peak usage hours and water supply shortages. *Id.*

210. U.S. Dep't of Energy, *supra* note 208.

211. *Id.*; Abrenio et al., *supra* note 28, at 7.

212. Nadya Bartol et al., The Bos. Consulting Grp., Ensuring Cybersecurity in the Electric Utility Industry 1 (2017), http://image-src.bcg.com/Images/BCG-Ensuring-Cybersecurity-in-the-Electric-Utility-Industry-Aug-2017_tcm9-167980.pdf. Utilities have experienced cyberattacks before, including the highly publicized Stuxnet attack. Bosch, supra note 208, at 1363, 1366. The Stuxnet attack infiltrated the command and control software for Iran's nuclear program, causing the program's centrifuges to self-destruct and resulting in physical damage. Abrenio et al., *supra* note 28, at 11; *see also* Zetter, *supra* note 29 (providing an overview of the Stuxnet cyberattack).

213. Abrenio et al., *supra* note 28, at 30.

that the North American Electric Reliability Corporation's (NERC)[214] standards create a duty between the government and utilities, but that the duty does not run to customers.[215] Federal regulation applies to the wholesale market while state utility commissions regulate retail power distribution.[216] Even when a utility contracts with a customer to provide a service for general purposes, such as the provision of electricity or water, it still may be insufficient under state law to create a duty to the customer for the interruption of the service.[217]

Utility companies face vendor management risk given the complexity of their supply chains. For example, an electric utility may potentially have hundreds of vendors involved in constructing and maintaining the generation, transmission, and distribution of electricity.[218] Supply chain management is critical to ensuring the cybersecurity of utilities.[219] Utilities have experienced an exponential growth in the use of IoT technologies developed by third parties.[220] A vulnerability in any of these devices places the rest of the network at risk,[221] and the risks would be compounded if vendors' technology or equipment are used at more than one plant.[222] Utilities should develop supply chain risk management programs to ensure that IoT technologies are designed and implemented securely, which may include establishing standardized security requirements, vendor assessments, and site visits.[223]

---

214. NERC is a not-for-profit international regulatory authority overseen by the U.S. Federal Energy Regulatory Commission. *About NERC*, N. Am. Electric Reliability Corp., http://www.nerc.com/AboutNERC/Pages/default.aspx (last visited Apr. 1, 2018). NERC is currently the only regulatory body with mandatory cybersecurity standards. Mission Support Center Analysis Report, *supra* note 45, at 23. NERC updated the standards governing electric utilities and operators, called the Critical Infrastructure Protection (CIP) Standards, which include access controls to cyber assets, electronic security perimeters, physical security, threat monitoring, personnel training, incident response reporting and planning, and recovery planning. *Id.*; *CIP Standards*, N. Am. Electric Reliability Corp., http://www.nerc.com/pa/Stand/Pages/CIPStandards.aspx (last visited Apr. 1, 2018). Given that NERC only recently incorporated cybersecurity standards into the CIP standards, there has been little case law or enforcement actions directly dealing with a utility's liability for failing to adhere to the cybersecurity standards. Abrenio, *supra* note 28, at 29. However, NERC has imposed penalties on entities for failing to comply with other aspects of the CIP standards, and it is reasonable to expect NERC to do the same with cybersecurity standards. *See id.*

215. Waldon v. Ariz. Pub. Serv. Co., 642 F. App'x 667, 669 (9th Cir. 2016); Abrenio et al., supra note 28, at 28–29. Courts have found that, in the absence of a contract with the utility, NERC's reliability standards do not give rise to a claim for negligence per se under state law. *Waldon*, 642 F. App'x at 669 (citing White v. S. Cal. Edison Co., 30 Cal. Rptr. 2d 431, 435 (Cal. Ct. App. 1994)).

216. *Waldon*, 642 F. App'x at 669.

217. *White*, 30 Cal. Rptr. 2d at 435–36.

218. Mission Support Center Analysis Report, *supra* note 45, at 15.

219. Bartol et al., *supra* note 211, at 4.

220. *Id.*

221. *Id.* at 2.

222. Mission Support Center Analysis Report, *supra* note 45, at 24.

223. Bartol et al., *supra* note 211, at 6.

VI. EUROPEAN REGULATORY LANDSCAPE

Europe has historically treated the protection of personal data as a fundamental right[224] and is in the process of implementing an aggressive regulatory approach to new technologies that capture the personal data of individuals residing in the European Union. These regulations will apply to the industrial IoT. While some U.S. regulators have delayed regulation to avoid stifling innovation for early stage technologies,[225] Europe has started down the path of using regulation to shape privacy and security at the outset of the IoT. These uncoordinated, and at times conflicting, approaches may create compliance difficulties and increase the costs for companies that operate across borders.

One of the most important European regulatory proposals on the horizon is the ePrivacy Regulation.[226] The ePrivacy Regulation would replace the current ePrivacy Directive, which was first enacted in 2002 and last revised in 2009 to protect the privacy and confidentiality of users of electronic communication services, namely through internet service and broadband providers.[227] Since the Directive has not kept pace with technological developments in electronic communication, the proposed ePrivacy Regulation would expand the coverage of the Directive and convert it to a regulation that becomes immediately enforceable in all member states. The ePrivacy Regulation would apply to "Over-the-Top" (OTT) communications services that are provided through internet-based services—such as web-based email or instant messaging services—that are not presently covered under the Directive.[228] The ePrivacy Regulation would require companies to keep electronic communications data confidential and prohibit any interference with the data, such as by "listening, tapping, storing, monitoring, scanning or other kinds of interception, surveillance or processing . . . by persons other than the end-users," except under certain circumstances, such as with consent of the end-user.[229]

The ePrivacy Regulation would even have implications for the industrial IoT.[230] European regulators recognize the growing importance of connected devices and

224. Council Regulation 2016/679, art. 51, 2016 O.J. (L 119) 1, 65 (EU), recital 1.

225. FTC IoT Guidance, *supra* note 80, at 48–49.

226. *See Proposal for a Regulation of the European Parliament and of the Council Concerning the Respect for Private Life and the Protection of Personal Data in Electronic Communications and Repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications)*, COM (2017) 10 final (Jan. 10, 2017) [hereinafter *ePrivacy Regulation*], https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52017PC0010.

227. *Id.* at recital 1.1; Council Directive 2002/58/EC, 2002 O.J. (L 201) (EC).

228. *See ePrivacy Regulation*, *supra* note 226, at recital 1.1.

229. *ePrivacy Regulation*, *supra* note 226, at arts. 5–6.

230. The potential scope of the ePrivacy Regulation is vast because it applies to any company providing electronic communications services to end-users in the EU, the use of such services, and the protection of information related to the terminal equipment of end-users in the EU. *Id.* at art. 3. Critics worry that it has the potential to apply to any business that communicates digitally with its customers. Jennifer Baker, *European Commission Proposes Formal ePrivacy Regulation*, IAPP: Privacy Tracker (Jan. 10, 2017), https://iapp.org/news/a/european-commission-proposes-formal-eprivacy-regulation/.

machines as a form of electronic communication and "want to promote a trusted and secure Internet of Things in the digital single market."[231] For this reason, regulators contemplate that the ePrivacy Regulation would apply to machine-to-machine communications over an electronic communications network.[232] However, the ePrivacy Regulation as currently proposed applies only to electronic communications services that are available to the public, not closed groups of end-users.[233] This means that the ePrivacy Regulation may not apply in certain industrial environments that are not designed to interact with the public, such as a manufacturing facility or an oil rig. But when designed to interact with the terminal equipment of an end user, such as a connected vehicle or smart medical device, other industrial IoT applications would be subject to the ePrivacy Regulation.

The high penalties proposed under the ePrivacy Regulation would raise the stakes for noncompliance. A company that violates the ePrivacy Regulation could be subject to administrative fines of up to ten million euros or up to two percent of annual worldwide turnover.[234] If the company violates the provisions of the ePrivacy Regulation related to confidentiality of communications, processing of electronic communications data, or time limits for erasure, the administrative fines could reach twenty million euros or up to four percent of annual worldwide turnover.[235]

In addition to the ePrivacy Regulation, the EU's General Data Protection Regulation (GDPR) goes into effect on May 25, 2018,[236] which is expected to affect companies using IoT technologies to collect and analyze data from end users.[237] The GDPR requires a company to have a lawful basis to process personal data[238] and grants enhanced rights to individuals,[239] such as the right to object to automated decision-making.[240] The GDPR also requires companies to implement technical and organizational measures to protect personal data collected through industrial IoT technologies.[241]

Complying with the GDPR is particularly difficult in an industrial IoT context. European regulators recognize the difficulties of complying with traditional notions of notice and consent when information is being gathered in less conventional ways

231. *ePrivacy Regulation*, *supra* note 226, at recital 12.

232. *Id.* at recital 12.

233. *Id.* at recital 13.

234. *Id.* at arts. 23.

235. *Id.*

236. Council Regulation 2016/679, art. 51, 2016 O.J. (L 119) 1, 65 (EU) [hereinafter "GDPR"].

237. Adam Finlay & Ruairi Madigan, *GDPR and the Internet of Things: 5 Things You Need to Know*, Lexology (May 26, 2016), https://www.lexology.com/library/detail.aspx?g=ba0b0d12-bae3-4e93-b832-85c15620b877.

238. GDPR, *supra* note 236, at arts. 6–7.

239. *Id.* at arts. 15–22.

240. *Id.* at art. 22.

241. *Id.* at art. 32.

through novel technologies.[242] Due to the growing significance of IoT technology to the digital economy, the Article 29 Data Protection Working Party, an advisory body made up of representatives of national Data Protection Authorities from each EU member state, issued an opinion in 2014 with recommendations for how companies using IoT technologies could meet notice and consent requirements under EU regulations.[243] For example, the Working Party recommended that IoT stakeholders aggregate data and delete raw data collected by IoT devices shortly after extracting it and that deletion should occur at the nearest point of collection of the data.[244]

A failure to comply with the GDPR carries potentially hefty fines of up to ten million euros or up to two percent of annual worldwide turnover.[245] The fine increases to twenty million euros or up to four percent of worldwide annual turnover for violations of processing principles or individuals' rights to object to the processing of their data.[246] Companies need to be aware that they are required to comply with the GDPR if their processing activities relate to the offering of goods or services to individuals in the EU or to monitoring the behavior of individuals if that behavior occurs within the EU, even if they are not established in the EU.[247]

VII. CONCLUSION

Use of data to improve industrial performance promises to bring fundamental changes to the operation of industry. The industrial IoT holds enormous potential to improve organizational processes, create efficiencies, generate revenues, and promote economic growth.[248] To achieve the full promise of the industrial IoT, industrial stakeholders, developers, and regulators must come together to overcome legal, regulatory, and technical hurdles.

As the landscape for the industrial IoT continues to develop, so do the operational risks, uncertainties, and liabilities faced by industrial companies. As more companies integrate industrial IoT technologies into their existing operations, they will grapple with the security, intellectual property, licensing, and litigation risks raised in this article. With no new U.S. laws or regulations governing the industrial IoT expected on the horizon,[249] these companies will have to address emerging security concerns and legal issues related to the industrial IoT with little guidance or precedent.

---

242. *See* Article 29 Data Protection Working Party, *Opinion 8/2014 on the Recent Developments on the Internet of Things*, 14/EN WP 223, at 7 (Sept. 16, 2014).

243. *Id*. at 14, 21. The European Data Protection Board will replace the Article 29 Working Party in May 2018 when the GDPR goes in effect. European Data Prot. Supervisor, Annual Report 2017, at 16 (2018).

244. *Id*.

245. GDPR, *supra* note 236, at art. 83(4).

246. *Id.* at art. 83(5).

247. *Id.* at art. 3.

248. *See* Paez & La Marca, *supra* note 1, at 31.

249. *See* FTC IoT Guidance, *supra* note 80, at 48–49.