Berkeley Technology Law Journal

Volume 31
Issue 2 *Annual Review 2016*

Article 24

9-25-2016

Internet of Things: Underlying Technologies, Interoperability, and Threats to Privacy and Security

Swaroop Poudel

Recommended Citation

Swaroop Poudel, *Internet of Things: Underlying Technologies, Interoperability, and Threats to Privacy and Security*, 31 Berkeley Tech. L.J. 997 (2016).

Link to publisher version (DOI)
http://dx.doi.org/https://doi.org/10.15779/Z38WW0V

INTERNET OF THINGS: UNDERLYING TECHNOLOGIES, INTEROPERABILITY, AND THREATS TO PRIVACY AND SECURITY

Swaroop Poudel†

After the Internet reached billions of people, followed by the explosive growth of smartphones and their applications, the next frontier in information technology is very likely the Internet of Things (IoT).[1] IoT comprises an evolving array of technologies that extend the idea of instantaneous connectivity beyond computers, smartphones, and tablets to everyday objects such as home appliances, cars, and medical devices. Applications have already appeared in our lives, but IoT has far from reached its potential. It promises the future development of many services. Cisco projects that fifty billion devices will be connected to the Internet by 2020,[2] and Strategy Analytics forecasts that the IoT market will be worth $242 billion in 2022.[3]

A current smart home IoT application, Nest's Thermostat, encapsulates some of the promises and technologies that undergird the concept of IoT.[4] First, Nest connects to the consumer's smartphone through an app so that the consumer can remotely regulate the temperature of her home.[5] Second, it has enhanced sensors that detect not only the current temperature but also when she walks in the room, as well as actuators that light up a panel when

DOI: http://dx.doi.org/10.15779/Z38PK26

† J.D. Candidate, 2017, University of California, Berkeley, School of Law.

1. *See* Press Release, *Gartner's 2014 Hype Cycle for Emerging Technologies Maps the Journey to Digital Business*, GARTNER, INC. (Aug. 11, 2014), http://www.gartner.com/newsroom/id/2819918 [https://perma.cc/48W3-4XFH] (ranking IoT at the top of hype cycle for emerging technologies and predicting a five to ten year full maturity period for the market).

2. Dave Evans, *The Internet of Things: How the Next Evolution of the Internet is Changing Everything*, CISCO, 3 (Apr. 2011), https://www.cisco.com/web/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf [https://perma.cc/DUF9-A9YY].

3. Press Release, *M2M Market Will Generate $242 Billion Revenue by 2022*, STRATEGY ANALYTICS (Jan. 8, 2014), http://strategyanalytics.com/default.aspx?mod=pressreleaseviewer&a0=5468 [https://perma.cc/BME4-V3AP].

4. *Meet the Nest Thermostat*, NEST, https://nest.com/thermostat/meet-nest-thermostat [https://perma.cc/SW6W-6A8Y].

5. *Id.*

she moves to show her the temperature and time.[6] Third, Nest features machine learning of her habits in order to automate temperature settings. For instance, by remembering the temperature she sets right before bedtime and after getting up from bed in the morning, it creates a temperature-setting schedule.[7] Similarly, it will learn to turn off the heat when she leaves home.[8]

The Nest thermostat is currently an example of a "vendor-specific closed-loop scheme" (that is, only other Nest products can connect with it), but IoT has the potential to unlock immense value when more devices become interoperable with each other.[9] For instance, the value to customers would significantly increase if third-party application developers could build on the current system to add services such as regulation of lighting and humidity. Similarly, if the smart home is connected to a smart car, then the smart home can turn up the heat when the car is about to approach home.

Consider another example that illustrates other potential uses and challenges of IoT: a connected health (or a smart health) application for smart phones and watches called Fido that is designed by a company named Fjord.[10] While current non-IoT devices can detect one's glucose level at a point in time and recommend an appropriate insulin dose, Fido promises several functionalities to better manage the chronic diabetic condition.[11] First, Fido is device-agnostic. That is, it will work on many devices such as smartphones and watches.[12] Second, it measures and records not just glucose level but also nutrition, stress level, sleep, and activity, and does so either automatically or through consumer input.[13] It also measures all of this data over long periods of time. This collection of a variety of data at a granular level via various sensors speaks to the enormous scale of IoT data over what computers can currently collect. Third, by aggregating data from several people, it can discern the pattern between glucose level and various

6. *Id.*
7. *Id.*
8. *Id.*
9. *See* GS1 US, *Comment Letter on FTC Seeking Input on Privacy and Security Implications of the Internet of Things*, 3 (July 25, 2013), https://www.ftc.gov/policy/public-comments/comment-00030-2 [https://perma.cc/2NDB-NZE5].
10. Eric Wicklund, *Analytics and mHealth Find Common Ground*, MHEALTHNEWS (Oct. 1, 2015), http://www.mhealthnews.com/news/analytics-and-mhealth-find-common-ground [https://perma.cc/FB48-KUAR].
11. Jeb Brack, *Platform Eyes Easier Diabetes Management for 400 Million Sufferers*, PSFK (Oct. 9, 2015), http://www.psfk.com/2015/10/diabetes-management-type-1-diabetes-platform-fjord-fido.html [https://perma.cc/GM4R-7DA2].
12. Wicklund, *supra* note 10.
13. *Id.*

consumer habits, and thus, suggest behavioral changes to help manage that glucose level.[14] This would not be possible without enhanced data analytics capabilities. Fourth, when a consumer's glucose level goes over a safe threshold, Fido can alert healthcare providers to enable a timely, life-saving intervention.[15] Fido shows the tremendous potential benefits of IoT, but also presents a sobering reminder of IoT's privacy and security implications. Health data is sensitive, and its granularity presents significant challenges to anonymizing personal information, thereby exposing consumers to privacy and data security risks.

Two conventional products, namely, home security systems and electronic toll collection, show how IoT differs from similar currently available products. A home security system utilizes various motion and sound sensors to detect intrusion into a home, and actuators to give automated alerts such as bells, sirens, and flashing lights.[16] Further, its components are interconnected through wired or wireless means.[17] Similarly, an electronic toll collection system such as E-ZPass uses RFID technology to authenticate a given vehicle and process automated payments.[18] What both of these systems do not have, however, is the "back-end information infrastructures necessary to create new services."[19] In other words, as this Note will explain later, there is no common services layer upon which to add or modify functionalities once the system is put in place.[20] Further, the fairly basic and limited data they store and process fail to capture the role of big data analytics in IoT.[21] At the same time, these examples illustrate that many of the technologies that enable IoT have been around for some time, and it is only the convergence of these disparate technologies as well as their rapid advancement that has helped create a vision for IoT.

14. Brack, *supra* note 11.

15. Wicklund, *supra* note 10.

16. *Security Alarm*, WIKIPEDIA, https://en.wikipedia.org/wiki/Security_alarm [https://perma.cc/36AN-5X7D].

17. *Id.*

18. Kantara Initiative, *Comment Letter on FTC Seeking Input on Privacy and Security Implications of the Internet of Things* (May 2013), https://www.ftc.gov/policy/public-comments/comment-00016-2 [https://perma.cc/G4MM-KCL4].

19. Ovidiu Vermesan et al., *Internet of Things Strategic Research Roadmap*, IOT EUROPEAN RESEARCH CLUSTER, 17 (2011), http://www.internet-of-things-research.eu/pdf/IoT_Cluster_Strategic_Research_Agenda_2011.pdf [https://perma.cc/GWC9-L2FX].

20. *See infra* Section I.A.

21. *See infra* Section I.B.

More generally, IoT has wide-ranging applications.[22] It is already deployed in products such as home thermostats (like Nest), health monitoring (via wearables such as FitBit), automobiles, and parking. More remarkably, IoT could potentially revolutionize diverse fields such as electric grids, water leakage detection, autonomous vehicles, traffic management, forest fire detection, agriculture, manufacturing, inventory management, and supply chain control.[23]

Part I of this Note defines IoT through a description of underlying technologies. Notwithstanding IoT's significant promise, there are two main issues that can obstruct the growth of this sector—lack of interoperability and threats to privacy and security. Parts II and III explain these issues and the regulatory response to date. An understanding of underlying technologies from Part I will equip the reader to see these issues in concrete terms. Lastly, Part IV argues that, while regulators should promote broad principles and remain watchful of risks developing in the IoT space, they should not impose excessive restrictions that may hinder the innovation, growth, and progress that IoT promises.

I. ARCHITECTURE AND ENABLING TECHNOLOGIES: DEFINING THE INTERNET OF THINGS

There is no universal definition of IoT because it is a nascent industry whose technology and participants are in a state of great flux.[24] But some of IoT's architectural models and enabling technologies point to a workable definition. This discussion will help show how privacy and security risks arise, as well as shed light on ways to achieve interoperability.

A. IOT ARCHITECTURE

Figure 1 is a visual representation of how different IoT components can fit in an overall architectural model. It illustrates how different IoT products

22. Perhaps the most talked about example of a future IoT product is a smart refrigerator, which keeps track of, for instance, the number of remaining eggs in it and alerts a consumer when eggs are about to run out. This smart refrigerator can even automatically place orders online, and if connected to a smart scale, warn the consumer of her most recent weight and BMI as she pulls out a pint of ice cream from the fridge. Patrick Thibodeau, *Explained: The ABCs of the Internet of Things*, COMPUTERWORLD (May 6, 2014), http://www.computerworld.com/article/2488872/emerging-technology-explained-the-abcs-of-the-internet-of-things.html [https://perma.cc/63Q8-JYML].

23. *See* Ian G. Smith et al., *The Internet of Things 2012: New Horizons*, IOT EUROPEAN RESEARCH CLUSTER, 35–39 (2012), http://www.internet-of-things-research.eu/pdf/IERC_Cluster_Book_2012_WEB.pdf [https://perma.cc/C8BP-QZ8M] (discussing potential applications of IoT).

24. *See* Thibodeau, *supra* note 22.

fit together and explains the relationship between the many different types of companies creating IoT products.[25] It also provides guidance as to how new technologies may get incorporated into the system.

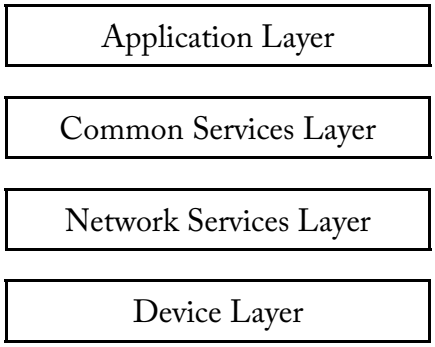

Figure 1: oneM2M Layered Model, Along With ITU's Device Layer

Two organizations created the models described here: oneM2M, an umbrella standards organization comprising several other standards bodies as well as vendors and service providers, and International Telecommunications Union (ITU), a United Nations agency for Information and Communication Technologies (ICTs).[26] oneM2M's model consists of three layers: application, common services, and network services.[27] The application layer contains the high-level programs and applications, along with business and operational logic.[28] The common services layer performs data storage and processing as well as other functions specific to applications, and the network services layer provides transport, connectivity, and service functions.[29] Along with the above three layers, ITU's model also includes the device layer, a fourth layer below the network layer.[30] The device layer comprises devices that upload information and receive commands via the network layer either directly or through gateways.[31] Here, gateways provide multiple interfaces and support protocol

25. *See* Kantara Initiative, *supra* note 18, at 1.

26. Roberto Minerva, Abyi Biru & Domenico Rotondi, *Towards a Definition of the Internet of Things (IoT)*, IEEE INTERNET INITIATIVE, 14–16 (May 27, 2015), http://iot.ieee.org/images/files/pdf/IEEE_IoT_Towards_Definition_Internet_of_Things_Revision1_27MAY15.pdf [https://perma.cc/85K7-GZRL] (describing the standard-setting organizations for IoT); *Overview of the Internet of Things*, ITU, 6–9 (June 15, 2012), https://www.itu.int/ITU-T/recommendations/rec.aspx?rec=y.2060 [https://perma.cc/9KMK-ARKV] [hereinafter Overview of IoT].

27. Minerva, Biru & Rotondi, *supra* note 26, at 14–16.

28. *Id.*

29. *Id.*

30. Overview of IoT, *supra* note 26, at 6–9.

31. *Id.*

conversion between devices connected through different means or between the device and network layers.[32]

To see how the four layers work, consider a connected health system.[33] In the device layer, data moves from various medical sensors attached to a patient to a monitoring hub or gateway at home via an unlicensed wireless link such as Bluetooth or Near Field Communication.[34] That information is then transmitted from the gateway through the network layer (typically a broadband network) to the cloud.[35] Tools for data storage and processing, which make up the service layer, reside in the cloud.[36] Finally, in the application layer, an application runs predictive analysis on all the data and notifies the patient's healthcare provider when anomalies appear.[37] In this example, risks to privacy or data security breach can occur within the devices or the monitoring hub (where data is stored before transmission to the cloud), during data transit to the cloud (that is, in the network), or in the cloud where data is stored and processed. Privacy and security are big issues that will be explored in greater detail in Part III.

The architectural model also explains the roles of different businesses in the interconnected IoT system and how businesses could achieve interoperability. The operator of a network (such as a broadband provider or other telecom) provides connectivity and related services to a service provider (like Google's cloud service), which provides common services to an application service provider (such as the company that sells the medical service to the customer), which in turn operates applications for the end user.[38] The oneM2M Initiative aims to achieve interoperability in the entire IoT system across industries.[39] oneM2M has recognized the common services layer as the bottleneck for interoperability.[40] The European Telecommunications Standards Institute (ETSI), a regional standards organization and contributor to oneM2M, is working to create a "horizontal

32. *Id.*

33. *See* AT&T, *Comment Letter on FTC Seeking Input on Privacy and Security Implications of the Internet of Things*, 5–7 (May 31, 2013), https://www.ftc.gov/policy/public-comments/comment-00004-2 [https://perma.cc/AG66-MZYM].

34. *See id.* at 5, 9.

35. *See id.* at 5.

36. *See id.*

37. *See id.*

38. *See id.* at 10–11.

39. *See id.* at 11; *The Interoperability Enabler for the Entire M2M and IoT Ecosystem*, ONEM2M, 13 (Jan. 2015), http://www.onem2m.org/images/files/oneM2M-whitepaper-January-2015.pdf [https://perma.cc/AT7R-QU8T].

40. *See* ONEM2M, *supra* note 39, at 9.

pipe scenario" in which applications across industries build on a common services layer and network elements.[41]

B. IOT'S ENABLING TECHNOLOGIES

Many technologies have converged to make IoT possible.[42] More specifically, advancements in microprocessors, sensors, and communication hardware typically found in IoT devices, along with big data analytics, the cloud, and algorithms to automate various ordinary processes have all made IoT a viable reality.[43] Other factors influencing the development of IoT include network technologies that link different devices as well as connect devices to a remote processor, the introduction of a new Internet communication protocol (IPv6), and more precise satellite GPS technology.

Sensors, such as cameras, thermometers, and pedometers, lie at the heart of an IoT system.[44] These collect varied information about the environment, such as mechanical data (position, force, pressure), thermal data (temperature, heat flow), electrostatic or magnetic field, radiation intensity (electromagnetic, nuclear), chemical data (humidity, ion, gas concentration), and biological data (toxicity, presence of bio organisms).[45] Sensors can work with actuators, output devices that implement decisions.[46] For example, an electronic jacket can have sensors that detect external temperature, and actuators that adjust the jacket's temperature.[47] Sensors can also combine to form useful applications. When a moisture sensor detects water on the basement floor and a temperature sensor in the main water pipe detects water flow (as the temperature lowers), this points to leakage.[48] The system can be set to trigger an automated valve shutoff when the sensors detect these two circumstances. Where the moisture sensor detects only water on the basement floor without the change in pipe temperature, it would not trigger any response because routine leakage from

41. Minerva, Biru & Rotondi, *supra* note 26, at 16.

42. *See, e.g.*, Eric A. Fischer, Cong. Research Serv., R44227, *The Internet of Things: Frequently Asked Questions*, 11–14 (Oct. 13, 2015), https://www.fas.org/sgp/crs/misc/R44227.pdf [https://perma.cc/M8EH-DJMB] (explaining the many technologies and potential pitfalls of their combination in IoT).

43. *See id.* at 2.

44. *See The Internet of Things*, ITU, 21 (Nov. 2005), https://www.itu.int/net/wsis/tunis/newsroom/stats/The-Internet-of-Things-2005.pdf [https://perma.cc/7SC6-V6YL] [hereinafter ITU—IoT].

45. *See id.*

46. *See id.*

47. *See id.*

48. Thibodeau, *supra* note 22.

heavy rainfall might cause water on the floor.[49] The burgeoning demand for microchips in the phone and tablet markets has led to cheaper and less power-intensive sensors.[50] While this holds significant promise for IoT, the ability of sensors to collect varied data also raises privacy and data security concerns.[51]

Beyond cheaper and better sensors, cheaper, faster, and more widely available broadband Internet connectivity drives IoT expansion.[52] Growing demand from Internet subscribers over the past years has driven substantial growth in the deployment of fixed line, cellular 3G/4G and LTE, power line, and fiber-optic networks, which have increased available bandwidth.[53] An IoT system can use these networks, for instance, to connect a smart home system to the cloud, which can process sensor data. These networks connect the device layer and the common services layer.

Similarly, various local communication methods are available to connect devices with the gateway or with other devices within the device layer. Typically, an IoT device will have a radio to send and receive wireless communications.[54] Some standards have been designed to provide Wi-Fi communication among devices over a broad geographic range, while other standards cover a short to medium range.[55] IoT wireless protocols are meant

49. *Id.* Combining sensor data from various sources to produce information that is greater than the sum of information from individual sources is called "sensor fusion." *Opinion 8/2014 on the on [sic] Recent Developments on the Internet of Things*, ARTICLE 29 DATA PROTECTION WORKING PARTY, 7 n.6 (Sept. 16, 2014), http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp223_en.pdf [https://perma.cc/NBK5-HMA8].

50. *See* Sir Mark Walport, *The Internet of Things: Making the Most of the Second Digital Revolution*, UK GOV'T OFF. FOR SCIENCE, 15 n.3 (Dec. 2014), https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/409774/14-1230-internet-of-things-review.pdf [https://perma.cc/LW7G-AM5X].

51. *Id.* at 16.

52. *Id.* at 15 n.8.

53. *Id.*; Bernadette Johnson, *How the Internet of Things Works*, HOWSTUFFWORKS, http://computer.howstuffworks.com/internet-of-things.htm/printable [https://perma.cc/LY6T-96XW].

54. *See* Thibodeau, *supra* note 22; Johnson, *supra* note 53.

55. Electronic Privacy Information Center (EPIC), *Comment Letter on FTC Seeking Input on Privacy and Security Implications of the Internet of Things*, 3–6 (June 1, 2013), https://www.ftc.gov/policy/public-comments/comment-00011-2 [https://perma.cc/7H62-UCLQ]. For example, the Worldwide Interoperability for Microwave Access (WiMAX) and 802.16 Wireless Metropolitan Network (WMAN) standards broadcast over several miles, and the 802.11p standard facilitates intelligent transport systems. Bluetooth and Radio Frequency Identification (RFID) communication technologies can offer a range from three to three hundred feet, whereas Near Field Communication (NFC) offers a much shorter range of up to four inches. Because RFID communication operates through

to operate on low power, use low bandwidth, and work on a mesh network.[56] In a mesh network, devices connect directly with one another to relay information, enabling the network to sprawl over a wide area even though a single device may transmit only up to 300 feet.[57] Mesh networks are also immune to the failure of any individual device.[58]

Advancements in the protocols used to assign Internet protocol (IP) addresses, specifically IPv6, and the satellite-based global positioning system (GPS) promise vast improvements in identifying and tracking IoT devices, but raise privacy and security concerns. Whereas the older version of the IP protocol, IPv4, ran out of its 2^{32} addresses in 2011, IPv6 offers 2^{128} unique addresses.[59] This enables each IoT device to have its own unique, persistent identifier, thereby enhancing identifying and tracking capabilities of devices across multiple networks as well as creating privacy and security ramifications.[60] Similarly, GPS can provide detailed three-dimensional location data (latitude, longitude, and altitude) precise to within 100 feet, time to within a millionth of a second, and velocity to within a fraction of a mile per hour.[61] This offers great tracking functionality, for instance, in Event Data Recorders (EDR) in cars, but it also has serious privacy implications.[62]

IoT is intimately connected to the notion of big data: collecting and storing a large amount and variety of granular data in real time, and using

---

tags, it also gives a device a unique identifier, which helps in tracking the location and status of the device. *Id.*

56. Thibodeau, *supra* note 22. The Z-Wave Alliance, Zigbee Alliance, and Insteon have developed wireless mesh IoT protocols, which are not directly interoperable, but can work together via hubs. *Id.*

57. *See id.*

58. *See id.*

59. EPIC, *supra* note 55, at 7–9.

60. *Id.*; *see* Thibodeau, *supra* note 22. Under IPv4, multiple devices in a local network connected to the same router share the same IP address while communicating in and out of the network, and have unique sub-addresses within the network. Consequently, individual devices "enjoy a certain degree of anonymity." EPIC, *supra* note 55, at 7. On the other hand, IPv6 obviates the need for devices to share an IP address (although periodically randomizing IP addresses and generating temporary addresses can still anonymize a device). *Id.* at 8. In a smart metering system, this means that IPv6 can help track individual appliances, but potentially also expose granular data on a customer's use of appliances to privacy and security threats. *Id.* at 11.

61. Global Positioning System Fact Sheet, LOS ANGELES AIR FORCE BASE (Jan. 19, 2009), http://www.losangeles.af.mil/library/factsheets/factsheet.asp?id=5325 [https://perma.cc/29KT-TUFW].

62. EPIC, *supra* note 55, at 10–12.

data analytics to reveal insights from these data.[63] Putting together all the data from the device layer in a big data "lake" enables its analysis in the context of other information, helping previously unseen linkages, patterns, and inferences emerge.[64] Interoperability of various IoT systems will allow for such pooling of data.[65] Society cannot realize IoT's full value proposition if sensor data languishes in information silos, accessible only to a few specialists.[66] At the same time, storage and network limitations render storing and transmitting all the data inefficient. Therefore, data management—determining "what type of data is important, what should be transmitted immediately, what should be stored and for how long, and what information should be discarded"—is essential.[67] Data management minimizes data stored and time stored, one of the principles advocated by the Federal Trade Commission (FTC) in order to mitigate privacy and data security risks in IoT.[68]

The development of cloud computing has been of paramount importance to big data and will play a major role in the IoT infrastructure. Instead of expanding their native infrastructures, many enterprises are moving the storage and processing of big data to the cloud for enhanced scalability and flexibility.[69] The cloud also provides the platform for third party app developers to build solutions, akin to an "app store" on mobile phones and mirroring oneM2M's vision of a common services layer.[70]

63. *See* Charles McLellan, *The Internet of Things and Big Data: Unlocking the Power*, ZDNET (Mar. 2, 2015), http://www.zdnet.com/article/the-internet-of-things-and-big-data-unlocking-the-power [https://perma.cc/74DW-6SKW].

64. *See* Drew Robb, *How IoT Will Change Big Data Analytics*, ENTERPRISE APPS TODAY (Nov. 17, 2014), http://www.enterpriseappstoday.com/business-intelligence/how-iot-will-change-big-data-analytics.html [https://perma.cc/L63S-N43C].

65. *See* Andy Vitus, *The California Drought and Standards of IoT*, TECHCRUNCH (Oct. 17, 2015), http://techcrunch.com/2015/10/17/the-california-drought-and-standards-of-iot [https://perma.cc/YE6L-9BF6].

66. Robb, *supra* note 64.

67. *Id.*

68. FTC, STAFF REPORT, *Internet of Things: Privacy & Security in a Connected World*, 33–36 (Jan. 2015), https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf [https://perma.cc/5D7F-F9EE].

69. *See* Kaushik Pal, *The Impact of Internet of Things on Big Data*, DATAINFORMED (Sept. 10, 2015), http://data-informed.com/the-impact-of-internet-of-things-on-big-data [https://perma.cc/2Z2B-2HN7].

70. *See* Sean Gallagher, *Machine Consciousness: Big Data Analytics and the Internet of Things*, ARS TECHNICA (Mar. 24, 2015), http://arstechnica.com/information-technology/2015/03/machine-consciousness-big-data-analytics-and-the-internet-of-things [https://perma.cc/6293-UPPR]. GE Software CTO envisions a "cloud operating system" for industrial

However, location-based or network latency issues can affect the cloud.[71] Some IoT systems will, therefore, need more computing power on the edge of the network, in what Cisco calls "fog" networking.[72] Fog networking will, for instance, enable an autonomous vehicle to receive signals from traffic lights, mapping programs, and other vehicles in real time.[73] Additionally, it will reduce data to a more manageable form, enhance reliability, and lower privacy and data security risks from the transmission of granular data over the network.[74]

Finally, automation is a major component of IoT's scalability and value proposition. As the number of connected devices rises, their added value will diminish if customers have to track and maintain all of their devices manually. As discussed earlier in this Part, devices can offload processing and automation capability to cloud-based software.[75] Alternatively, a sensor web combines "distributed network"—sharing of data collected by all sensors across the entire network—and "embedded intelligence"—the system's acting on its own without communicating to an end user or an external control system for analysis and decision-making.[76]

Irrespective of the loci of intelligence, IoT algorithms can extend beyond simple if-then routines of past embedded computing to machine

analytical apps whereby companies can control access to their sensor data while leveraging analytic software written by third party developers. *Id.*

71. McLellan, *supra* note 63.

72. *Fog Computing and The Internet of Things: Extend the Cloud to Where the Things Are*, CISCO (2015), http://www.cisco.com/c/dam/en_us/solutions/trends/iot/docs/computing-overview.pdf [https://perma.cc/Q7YA-5N74] (describing fog computing: "[t]he fog extends the cloud to be closer to the things that produce and act on IoT data. These devices, called fog nodes, can be deployed anywhere with a network connection.").

73. *See* Robb, *supra* note 64. Likewise, in industrial applications, devices often need to communicate and make decisions locally, as in Airbus's vision of using data analytics in tracking the performance of a system where intelligent tools will replace humans in manufacturing planes. GE similarly uses local analytics to change the configuration of its wind turbines based on sensor data on, for instance, wind gust. Sean Gallagher, *The Future Is the Internet of Things—Deal with It*, ARS TECHNICA (Oct. 29, 2015), http://arstechnica.com/unite/2015/10/the-future-is-the-internet-of-things-deal-with-it [https://perma.cc/Z4C3-UAQZ].

74. *See* Gallagher, *supra* note 73. Gartner uses the term "distributed approach to data center management" whereby multiple "mini-data centers" perform initial processing and forward relevant data over WAN links to a centralized location for further analysis. *See* Press Release, *Gartner Says the Internet of Things Will Transform the Data Center*, GARTNER, INC. (Mar. 19, 2014), http://www.gartner.com/newsroom/id/2684616 [https://perma.cc/PYE9-FNVY].

75. Johnson, *supra* note 53.

76. ITU—IoT, *supra* note 44, at 23–24.

learning, which is a form of artificial intelligence.[77] Machine learning can enable recognizing patterns from data, making predictions, and continually improving the algorithm to produce the most efficient responses.[78] It is particularly useful when it is not possible to foresee every possible future scenario in an IoT application. For instance, because one cannot predict every circumstance on the road, algorithms in autonomous vehicles are expected to rely on machine learning and other forms of artificial intelligence.[79]

C. DEFINING IOT

There is no hard and fast definition of IoT. According to Cisco, IoT is simply a point in time when more devices are connected to the Internet than are people.[80] This occurred in 2010—12.5 billion connected devices vis-à-vis 6.8 billion people—thanks in large part to the explosive growth of smartphones and tablets.[81] While this definition captures the exponential rise of Internet-connected devices, it fails to encapsulate the characteristics of many emerging technologies that substantiate the concept of connecting objects beyond phones, tablets, and computers to the Internet.

Other definitions emphasize the various technologies that enable IoT. Underscoring the role of sensors and Internet connectivity, the Institute of Electrical and Electronics Engineers (IEEE), the world's largest Standard Setting Organization (SSO), defines IoT as "a network of items—each embedded with sensors—which are connected to the Internet."[82] Similarly, according to the Organization for the Advancement of Structured Information Standards (OASIS), a consortium that works to advance open standards for the information society, IoT is a "system where the Internet is connected to the physical world via ubiquitous sensors."[83] Taking a different approach, ETSI highlights the significance of automation in defining a concept similar to IoT, "machine to machine (M2M) communication:" "communication between . . . entities that do not

77. *See* Johnson, *supra* note 53.

78. *The Economist Explains: How Machine Learning Works*, ECONOMIST (May 13, 2015), http://www.economist.com/node/21651052/print [https://perma.cc/8WNA-VCGU].

79. For a more in-depth discussion on autonomous vehicles, see Jessica Brodsky, Note, *Autonomous Vehicle Regulation: How an Uncertain Legal Landscape May Hit the Brakes on Self-Driving Cars*, 31 BERKELEY TECH. L.J. 851 (2016).

80. Evans, *supra* note 2, at 2.

81. *See id.* at 3.

82. Minerva, Biru & Rotondi, *supra* note 26, at 10.

83. *Id.* at 21.

necessarily need any direct human intervention. M2M services intend to automate decision and communication processes."[84]

According to the ITU, IoT embodies the vision of a "ubiquitous network," connected "anytime, anywhere, by anyone and anything."[85] In other words, IoT allows "people and things to be connected anytime, anyplace, with anything and anyone, ideally using any path/network and any service."[86] This way of viewing IoT speaks to its constituent elements, reach, and vision, and puts IoT in the context of earlier achievements in computing; that is, after mobile Internet expanded "anytime" connectivity to "anyplace," IoT promises to extend it to "anyone" and "anything."[87] It also hopes to attain interoperability in networks and services.

II. INTEROPERABILITY

The IoT industry is projected to be worth hundreds of billions of dollars in the future.[88] Although vendors will offer IoT products that are vertically integrated to varying degrees, no one company can supply all of IoT's constituent parts and technologies. Likewise, the lack of a common services layer will hinder horizontal interoperability, that is, prevent application developers from utilizing existing IoT infrastructure to offer applications to end customers. Thus IoT may not become the massive industry it is projected to become unless its many constituting devices can interoperate, or communicate with each other. In fact, oneM2M argues that market projections of growth of IoT are unrealistic absent a global standardized platform.[89]

The dual standards in videocassette recorders (VCRs), Sony's Betamax and JVC's VHS, present a classic illustration of the value of standards.[90] As the two companies jostled for market share, confusion among vendors, video shop rentals, and customers followed.[91] Vendors manufactured VCRs in one or both formats and rental shops stocked two copies of each movie title—a waste of resources in addition to dual research and development and

84. *Id.* at 12.
85. *See* ITU—IoT, *supra* note 44, at 3.
86. Vermesan et al., *supra* note 19, at 12.
87. *See* ITU—IoT, supra note 44, at 3.
88. *See* STRATEGY ANALYTICS, *supra* note 3.
89. oneM2M, *supra* note 39, at 2.
90. *See* Andrew Updegrove, *The Essential Guide to Standards: What (and Why) Is an SSO?*, CONSORTIUMINFO (2007), http://www.consortiuminfo.org/essentialguide/whatisansso.php [https://perma.cc/3WJD-5BLX].
91. *Id.*

marketing by Sony and JVC.[92] The ambiguity also stunted the growth of the entire VCR ecosystem.[93] VHS eventually prevailed over Betamax even though many believed that the latter was a technologically superior product.[94] A standard in VCR technology from the start would have limited inefficiencies and propelled the growth of related industries.[95] Further, if the standard had emerged from collaboration between competitors in a standards organization, they could have pooled their knowhow to produce something even technologically superior.

IoT platforms are currently highly fragmented.[96] The current lack of standards remains a significant hurdle to unlocking significant economic value from IoT.[97] Like during the VCR standards battle, vendors and end users could be delaying investments—even though they see value in using IoT—because they fear making irreversible investments in the standard that loses out in the end. This problem is particularly acute in a system such as smart meters, where it takes twenty to thirty years to recoup initial investment outlays.[98] Utility service providers will, therefore, need assurances that network interfaces will be stable and device software will be manageable and upgradable. More broadly, standards that provide common service layer capabilities and open interfaces will help "reduce investments, time-to-market, development and on-boarding costs, and facilitate management of devices and applications."[99] In order for IoT to become ubiquitous, applications should be "abstracted from the underlying access networks and technologies," which will require interoperability between "devices, platforms, data formats, protocols, and applications."[100] Standards will, thus, enhance scalability and flexibility in IoT applications.[101]

Indirect network effects are at play in the IoT market; that is, the more widely end users adopt a company's platform, the more vendors and developers are drawn to the platform and vice versa. In such a market, a company that eventually owns the dominant platform will obtain a tremendous monopoly advantage. Given the likely exponential growth of the IoT market, the potential rewards are, thus, astronomical. However,

92. *Id.*
93. Sangin Park, *Quantitative Analysis of Network Externalities in Competing Technologies: The VCR Case*, 86 REV. ECON. & STATISTICS 937, 939 (2004).
94. Updegrove, *supra* note 90.
95. *See* Park, *supra* note 93, at 939.
96. *See* oneM2M, *supra* note 39, at 13.
97. *See id.* at 2; Walport, *supra* note 50, at 8, 16.
98. *See* oneM2M, *supra* note 39, at 6.
99. *Id.* at 6.
100. *Id.*
101. *See id.*

because there is currently no common dominant standard, the IoT market could evolve in different ways. In their work on competition in standard markets, economists Stanley M. Besen and Joseph Farrell outline three different scenarios that apply to the IoT ecosystem: (1) Tweedledum and Tweedledee, where firms choose incompatibility and race to make their platform dominant; (2) Battle of the Sexes, where firms agree to have a common standard, but push for their own standard or for a standard that is favorable to their firm; and (3) Pesky Little Brother, where the dominant firm attempts to exclude the smaller firm from its platform, but the smaller firm tries to make its product compatible with the dominant firm's platform.[102]

Today's fragmented IoT market shows signs of each of the three scenarios described above. Various strategies mark the Tweedledum and Tweedledee scenario. Firms can attempt to build an early lead, for instance, with companies like Nest, IBM, and AT&T coming up with newer and improved products to gain traction in the market.[103] In the IoT market characterized by indirect network effects, firms can also try to get ahead by opening up platforms to application developers, as Intel did in December 2014.[104] Yet another way to compete in the platform race is by making product preannouncements to keep customers away from competitors' platforms.[105] For instance, Orange demonstrated its intentions to be the dominant network operator of IoT in France by announcing its plans to build a Low Power Wide Area (LPWA) network that covers the entirety of metropolitan France.[106] Nest has similarly announced a certification program for its Thread platform in the near future.[107]

---

102. Stanley M. Besen & Joseph Farrell, *Choosing How to Compete: Strategies and Tactics in Standardization*, 8 J. ECON. PERSPECTIVES 2, 121–29 (1994).

103. *See id.* at 122; NEST, *supra* note 4; Jennifer Booton, *IBM Launches Internet of Things Division*, MARKETWATCH (Sept. 14, 2015), http://www.marketwatch.com/story/ibm-launches-internet-of-things-division-2015-09-14 [https://perma.cc/5ZWG-XXCV]; Stacey Higginbotham, *AT&T's Plan for the Internet of Things Goes Way Beyond the Network*, FORTUNE (Sept. 15, 2015), http://fortune.com/2015/09/15/att-internet-of-things [https://perma.cc/5W97-HFA8].

104. *See* Besen & Farrell, *supra* note 102, at 122–23; Aaron Tilley, *Intel Releases New Platform to Kickstart Development in the Internet of Things*, FORBES (Dec. 9, 2014), http://www.forbes.com/sites/aarontilley/2014/12/09/intel-releases-new-platform-to-kickstart-development-in-the-internet-of-things/#614684fc1028 [https://perma.cc/2VN3-EE8S].

105. *See* Besen & Farrell, *supra* note 102, at 123–24.

106. *Orange Deploys a Network for the Internet of Things*, ORANGE (Sept. 18, 2015), http://www.orange.com/en/Press-and-medias/press-releases-2016/press-releases-2015/Orange-deploys-a-network-for-the-Internet-of-Things [https://perma.cc/9KLP-EF4V].

107. Colin Neagle, *A Guide to the Confusing Internet of Things Standards World*, NETWORK WORLD (July 21, 2014), http://www.networkworld.com/article/2456421/

IoT-related standardization efforts at various consortia exemplify both Battle of the Sexes and Tweedledum and Tweedledee scenarios. Within a consortium, companies can compete with each other to use their technologies in the standard. At the same time, more than one consortium can work on a standard that attains the same goal, which results in a race to make their respective standards dominant. There is a publicly acknowledged competition between two service-layer platforms developed by the AllSeen Alliance—comprising Qualcomm, Cisco, Microsoft, LG, and HTC—and the Open Internet Consortium—comprising Intel, Atmel, Broadcom, Dell, Samsung, and Wind River.[108] Overall, the IoT platform standard market is fragmented, with several competing consortia trying to develop their own standards.[109] As an example of a Pesky Little Brother scenario, while Apple has allowed app developers and hardware manufacturers to build on its proprietary HomeKit platform, its insistence on cutting-edge encryption keys and chips used by Wi-Fi and Bluetooth devices has effectively excluded the developers.[110]

Going forward, the IoT market may experience persistent platform fragmentation. This will likely hinder full realization of IoT's value and retard the adoption of IoT. Alternatively, competition between standards may eventually lead to the rise of *de facto* dominant standards in different IoT segments.[111] However, as in the VCR standards battle, the best technologies may not win. Therefore, the best way forward may be to foster cooperation between competitors in developing various standards. Over time, when the business models of various IoT vendors crystallize and the dimensions of competition become clear, the industry may witness such broad standardization efforts, as when the establishment of the Internet in the 1990s led to the adoption of the World Wide Web.[112]

---

internet-of-things/a-guide-to-the-confusing-internet-of-things-standards-world.html [https://perma.cc/TKQ5-RW6H].

108. *Id.* While opening its platform to the open source community for collaboration, the OIC has expressed distrust with Qualcomm's intentions. *Id.* Similarly, Qualcomm has publicly denounced OIC's spurn of its platform. *Id.*

109. *See id.*

110. Christopher Null, *The State of IoT Standards: Stand By for the Big Shakeout*, TECHBEACON (Sept. 2, 2015), http://techbeacon.com/state-iot-standards-stand-big-shakeout [https://perma.cc/QA42-DK6R].

111. *See* Robert S. Sutor, *Open Source vs. Open Standards*, http://www.sutor.com/c/essays/osvsos [https://perma.cc/7W45-7E22].

112. *See* Direct Marketing Association, *Comment Letter on FTC Seeking Input on Privacy and Security Implications of the Internet of Things*, 2 (June 1, 2013), https://www.ftc.gov/policy/public-comments/comment-00010-2 [https://perma.cc/KN2F-GJE2].

III. THREATS TO PRIVACY AND SECURITY

The two biggest threats to the widespread adoption of IoT are privacy and security.[113] Consumers vote with their feet when it comes to protecting their data.[114] Given the likely ubiquity of IoT devices and the volume and granularity of sensor data collected, transmitted, and stored, IoT will magnify the types of privacy and security risks that already accompany the traditional Internet. But some privacy and security issues are particular to IoT.

A. PRIVACY

Sensors can collect a treasure trove of sensitive information about people, either directly or indirectly through inferences made from data over time.[115] For example, simple movement data from the accelerometer and the gyroscope contained in most smartphones can help decipher an individual's driving habits.[116] It can also help infer one's level of relaxation and, if supplemented by heart-sensor data, portray stress levels and emotions.[117] More generally, IoT devices can enable inferences about "a user's mood; stress levels; personality type; bipolar disorder; demographics (e.g., gender, marital status, job status, age); smoking habits; overall well-being; progression of Parkinson's disease; sleep patterns; happiness; levels of exercise; and types of physical activity or movement."[118] Left unchecked, IoT devices could allow intrusive surveillance into the private spheres of individuals' lives. Just as the widespread use of CCTV has influenced people's behavior in public spaces, IoT may pressure people to avoid behavior that can be perceived as anomalous even in the comfort of their homes.[119]

Unauthorized people may also use IoT data in unauthorized ways. While rich data created by the IoT ecosystem can lead to better credit, insurance, and employment decisions, its use without consumers' knowledge and consent can be harmful.[120] For instance, insurers could use

113. *See* Walport, *supra* note 50, at 6.

114. FTC, *supra* note 68, at 51–52.

115. Scott R. Peppet, *Regulating the Internet of Things: First Steps Toward Managing Discrimination, Privacy, Security, and Consent*, 93 TEXAS L. REV. 85, 113 (2014).

116. Article 29 Data Protection Working Party, *supra* note 49, at 7.

117. Peppet, *supra* note 115, at 121.

118. *Id.* at 115–16.

119. Article 29 Data Protection Working Party, *supra* note 49, at 8; *see also* Zygmunt Bauman & David Lyon, Liquid Surveillance (2013); Neil M. Richards, *The Dangers of Surveillance*, 126 HARV. L. REV. 1934 (2013).

120. Peppet, *supra* note 115, at 125–26.

Fitbit data to charge higher premiums to people with higher perceived health risks. A consumer's right to challenge accuracy in consumer reports under the Fair Consumer Reporting Act (FCRA) is inadequate here because sensor data is hardly inaccurate, and FCRA does not apply to specious inferences drawn from such accurate data.[121] FCRA also spares companies collecting data and conducting analytics in-house.[122] Similarly, even though Title VII of the Civil Rights Act prohibits various forms of discrimination, creditors, insurers, and employers can make inferences from sensor data to create proxies for race, gender, disability, or other protected classes.[123]

Further, IoT data largely breaks down the distinction between personal and nonpersonal information.[124] Comprising granular data with many variables, sensor data can enable someone with knowledge of certain attributes of a person to identify them, even without their personally identifiable information (PII)—examples of PII include name, social security number, telephone number, and address.[125] For example, Fitbit's movement data can reveal someone's gait.[126] Someone who knows a person's gait could, thus, identify that person and gain access to the rest of his or her Fitbit data.[127] Hence, data not previously considered personally identifiable information could now enable the re-identification of individuals in the IoT context, rendering the anonymizing of IoT data with de-identification and data aggregation ineffective.[128] Moreover, various existing and proposed state laws mandate notification upon breach of only personal data and have more stringent security requirements for personal data than for nonpersonal data.[129] This blurring of lines between personal and nonpersonal data will, in effect, weaken these laws.[130]

---

121. *Id.* at 128 (explaining that "[a]ccuracy, however, is really not the problem with Internet of Things sensor data . . . What is more questionable are the inferences drawn from such data. The FCRA does not reach those inferences, however. It applies to the underlying 'inputs' into a credit, insurance, or employment determination, not the reasoning that a bank, insurer, or employer then makes based on those inputs.").

122. *Id.* at 127.

123. *Id.* at 124–25.

124. *Id.* at 129–31.

125. *Id.* at 132.

126. *Id.* at 129.

127. *Id.*

128. *Id.*

129. *Id.* at 132–33. For a more in-depth discussion of data breaches and security breach notification laws, see Yasmine Agelidis, Note, *Protecting the Good, the Bad, and the Ugly: "Exposure" Data Breaches and Suggestions for Coping with Them*, 31 BERKELEY TECH. L.J. 1057 (2016).

130. *Id.*

B. SECURITY

Increased reliance upon IoT heightens both the risk of data breaches and physical harm to users of IoT systems or devices.[131] Each additional IoT device represents another point of vulnerability for intruders to access information.[132] A connected device can be an entry point for an attack on an entire network or other connected systems.[133] As a case-in-point from a non-IoT system, during the theft of forty million credit card numbers and infiltration of Target's computer system in 2013, attackers exploited security flaws in a contractor's computer system that was connected to Target's computer system for the purposes of "electronic billing, contract submission, and project management."[134] Further, IoT can pose a direct threat to people's physical safety through manipulation of device functions or tracking of user's location.[135] As examples, a hacker once exploited vulnerabilities of a baby monitoring device to shout at a sleeping toddler, and a group of researchers were able to control the steering and braking of a connected car by hacking it remotely.[136]

In addition to security risks emerging from communication links and storage infrastructure, IoT devices are inherently vulnerable for many reasons. First, manufacturers of these devices—primarily consumer goods companies—are inexperienced in data security issues relative to software or hardware firms.[137] Second, the devices' compact form and low battery life do not lend themselves to the high processing power that is "needed for robust security measures such as encryption."[138] Third, it is hard to periodically update or patch these devices with security fixes, thereby exposing them to threats not existing or contemplated at the time of their manufacture.[139]

---

131. *See* Jim Snell & Christian Lee, *The Internet of Things Changes Everything, or Does It?*, 32 COMPUTER & INTERNET LAWYER 2 (2015).

132. FTC, *supra* note 68, at 11.

133. *Id.* at 11–12.

134. Paul Ziobro, *Target Breach Began with Contractor's Electronic Billing Link*, WALL ST. J. (Feb. 6, 2014), http://www.wsj.com/articles/SB10001424052702304450904579367391844060778 [https://perma.cc/ZJ8H-SCRR].

135. FTC, *supra* note 68, at 12–13.

136. Andy Greenberg, *How Hackable is Your Car? Consult This Handy Chart*, WIRED (Aug. 6, 2014), http://www.wired.com/2014/08/car-hacking-chart [https://perma.cc/G5P3-E2A2]; *Home, Hacked Home: The Perils of Connected Devices*, ECONOMIST (July 12, 2014), http://www.economist.com/news/special-report/21606420-perils-connected-devices-home-hacked-home [https://perma.cc/E9DZ-E38F].

137. Peppet, *supra* note 115, at 135.

138. *Id.*

139. *Id.* at 135–36.

Moreover, lack of coordination among different stakeholders in the IoT ecosystem hampers not only interoperability but also security. There is a divergence of interests in the IoT ecosystem: for instance, while a telecom operator primarily wants to ensure network availability, a customer enterprise prioritizes data protection, and an IoT provider wants to ensure uptime.[140] Failure to coordinate technical design with implementation can also give rise to weak points, with "the level of security provided by the weakest component."[141] According to oneM2M, "the huge diversity of . . . IoT device types, their different capabilities and the range of deployment scenarios makes security a unique challenge for the . . . IoT industry."[142] For example, most sensors available today do not support encryption because the devices have limited battery power, and therefore, insufficient computing resources.[143]

C. REGULATORY RESPONSE TO DATE

The FTC proposed best practices to minimize privacy and security risks in its IoT report published in January 2015.[144] Recognizing that the IoT industry is still at an early stage with great potential for innovation, it opposes enacting IoT-specific legislation.[145] The FTC's recommendations consist of: (1) data security, (2) data minimization, and (3) notice and choice.[146]

The standard for data security is reasonable security, which depends on "the amount and sensitivity of data collected, the sensitivity of the device's functionality, and the costs of remedying the security vulnerabilities."[147] The FTC report makes several specific recommendations to companies developing IoT products. It advocates implementing "security by design," that is, building security into the devices at the outset;[148] promoting personnel policies to ensure prioritization of security needs;[149] and ensuring that third party service providers to whom the company has outsourced work maintain reasonable security.[150] For systems with significant risk, the report recommends adopting a "defense-in-depth" approach that considers

140. oneM2M, *supra* note 39, at 12.
141. Article 29 Data Protection Working Party, *supra* note 49, at 9.
142. oneM2M, *supra* note 39, at 12.
143. *See* Article 29 Data Protection Working Party, *supra* note 49, at 9.
144. *See* FTC, *supra* note 68, at i.
145. *Id.* at 48–49.
146. *See id.* at 27–46.
147. *Id.* at 27–28.
148. *Id.* at 28.
149. *Id.* at 29.
150. *Id.* at 30.

security measures at all levels, for instance, using data encryption in both transit and storage, instead of relying on consumers' passwords.[151] It also recommends using strong authentication to permit IoT devices to interact with other IoT devices and systems while not unduly hindering the device's usability, monitoring products through the life cycle, providing security updates, and patching known vulnerabilities after the sale of the devices.[152]

Data minimization encompasses reasonable limits on both collection and retention of data.[153] The FTC report also advocates a privacy-by-design approach whereby the company evaluates its data needs—"what types of data it is collecting, to what end, and how long it should be stored."[154] It also recommends considering whether a company can provide the same services with less granular data, for example, using zip codes instead of precise geographical location.[155] When de-identification is possible and de-identified data serves business needs, the report suggests that companies maintain data in de-identified form and publicly commit to not re-identify data.[156] At the same time, it acknowledges the importance of maintaining flexibility in the data minimization framework so as not to foreclose future innovations based on data they do not use today.[157]

The notice and choice framework advocated by the FTC allows a company to collect sensitive personal information with the express consent of consumers.[158] However, such consent is not required if data can be effectively and immediately de-identified, or if its collection and use is consistent with the context of a transaction or the relationship between the company and the customer.[159] To illustrate, a smart oven vendor that also offers an app to turn the oven on remotely and specify its temperature need not seek consumers' consent to use oven-usage information to improve the sensitivity of the oven's sensors or recommend related products to consumers.[160] On the contrary, the vendor would need consumers' consent to sell this data to a data broker or an advertisement network.[161] The report refrains from embracing a full use-based framework not in the least because

151. *Id.*
152. *Id.* at 31–32.
153. *Id.* at 33–34.
154. *Id.* at 36.
155. *Id.*
156. *Id.* at 36–37.
157. *Id.* at 38–39.
158. *Id.* at 39–40.
159. *Id.* at 40, 43.
160. *Id.* at 40–41.
161. *Id.*

the authority—either based on legislation or a multi-stakeholder code of conduct—on what constitutes a beneficial or harmful use of data is unclear.[162]

In order for a notice and choice framework to work, a user's consent should be meaningful and well-informed.[163] However, consent is hard to achieve in IoT devices, which are "often small and screen-less, and lack an input mechanism like a touch screen or keyboard."[164] Further, information related to privacy and data security is often only available on manufacturers' websites, without means for consumers to locate it.[165] When it can be located, it may be incomplete or vague.[166] For instance, many of these online privacy and security policies do not make it clear who owns the data collected by IoT devices, whether data is stored on the device or a remote server, what measures are employed to prevent security breaches, what data is collected, what constitutes personal and nonpersonal information and how they are treated differently, and whether consumers can access, modify, and delete raw data.[167]

In order to effectuate meaningful consent, the FTC recommends providing consumers options such as choice at the point of sale or set-up, choice through the website interface that can be accessed via code on the device, choice through a dashboard, and tutorials.[168] Companies can also offer general privacy menus along with an explanation of each privacy setting, or alternatively, personalize default privacy choices based on expressed past preferences.[169] While FTC recognizes that there cannot be a one-size-fits-all approach to acquiring consent, it cautions that privacy choices "should be clear and prominent, and not buried in lengthy documents."[170]

In addition to these best practice recommendations, § 5 of the Federal Trade Commission Act authorizes the FTC to bring an action against a company in response to that company's "unfair or deceptive acts or practices."[171] This gives limited authority to the FTC.[172] While the

162. *Id.* at 44–46.
163. *See* Article 29 Data Protection Working Party, *supra* note 49, at 7.
164. Peppet, *supra* note 115, at 140.
165. *Id.* at 141.
166. *See id.* at 142–45.
167. *See id.* at 144–45.
168. FTC, *supra* note 68, at 41–42.
169. *Id.* at 42.
170. *Id.* at 41, 43.
171. 15 U.S.C. § 45(a).
172. *See* Peppet, *supra* note 115, at 136–37.

"deception" prong requires a company's violating its own statements to consumers, the "unfairness" prong requires an injury to consumers through a violation of public policy.[173] FTC's complaint against TRENDnet, and its eventual settlement, marks the only IoT-related case thus far where the FTC invoked its § 5 authority.[174] TRENDnet marketed its Internet-connected cameras for various purposes including home security and baby monitoring, promising that the cameras were secure.[175] However, the company stored and transmitted over the Internet unencrypted login credentials and failed to test consumers' privacy settings.[176] Hackers were, therefore, able to access live video feeds from these cameras.[177]

Likewise, although forty-six states have enacted statutes requiring companies to disclose data breaches, they only cover variations of what has historically been considered personal information, leaving out a vast amount of IoT sensor data that can be used to identify individuals.[178] In response to these regulatory gaps, the FTC has called for general, technology-neutral data security and privacy legislation, which would apply to IoT but would not be specific to IoT.[179] This law would cover both personal data as well as device functionality, clarify when companies should give privacy notices and offer choices about data collection and use, and require companies to disclose a data breach.[180] This law could also articulate what constitutes a beneficial or harmful use of data, and, thus, help implement use-based restrictions of IoT data.[181]

The Article 29 Working Party ("Article 29"), an independent European advisory body on data protection and privacy, has also published best practices recommendations in its September 2014 IoT report.[182] The report acknowledges IoT's significant benefits, but also stresses the need to respect

173. *Id.*

174. *See* In the Matter of TRENDnet, Inc., 122 F.T.C. 3090 (Feb. 7, 2014) (FTC complaint), https://www.ftc.gov/system/files/documents/cases/140207trendnetcmpt.pdf [https://perma.cc/LVV6-VPYD]; PRESS RELEASE, *MARKETER OF INTERNET -CONNECTED HOME SECURITY VIDEO CAMERAS SETTLES FTC CHARGES IT FAILED TO PROTECT CONSUMERS' PRIVACY*, FED. TRADE COMMISSION (Sept. 4, 2013), https://www.ftc.gov/news-events/press-releases/2013/09/marketer-internet-connected-home-security-video-cameras-settles [https://perma.cc/B5HH-BK47].

175. FED. TRADE COMMISSION, Press Release, *supra* note 174.

176. *Id.*

177. *Id.*

178. *See* Peppet, *supra* note 115, at 137–39.

179. *See* FTC, *supra* note 68, at 48–52.

180. *Id.*

181. *Id.*

182. *See* Article 29 Data Protection Working Party, *supra* note 49.

the attendant privacy and security challenges.[183] Compared to the FTC's recommendations, Article 29's recommendations are more numerous, more specific, and tailored to many IoT stakeholders.[184] For instance, it recommends that OS and device manufacturers provide users a user-friendly interface to access personal data;[185] that application developers frequently warn users that sensors are collecting data;[186] that social platforms ask users to decide on publication on social platforms by default;[187] that users of IoT devices inform non-user data subjects about the presence of devices and the type of data being collected;[188] and that standardization bodies promote interoperable and clear data formats.[189]

IV. CONCLUSION AND POLICY IMPLICATIONS

In light of the huge potential of the IoT industry to create a positive impact in the world, but also to pose threats to privacy and security, the big question is the appropriate role of the government. IoT is an evolving industry, so any technological mandate can favor one emerging technology over the other when their relative merits are still unclear. Particularly because it is the convergence of many technologies that has made IoT possible, it is also hard to foresee the many uses of IoT. Further, consumers have different and evolving privacy preferences and, if well informed, can weigh risks and benefits to make appropriate choices. This favors industry self-regulation through representation of various stakeholders over government involvement. However, reliance on consumer education or vigorous participation by privacy advocates is often unrealistic. In the face of these uncertainties, the best regulatory approach going forward would be to observe market dynamics and self-regulatory efforts, promote broad principles, and take a wait-and-see approach. Regulators should still monitor the development of known threats and emergence of unknown threats.

Likewise, a lack of interoperability may stunt IoT's growth. Realizing this, the UK Government Office for Science recommends using government's technology procurement policies to encourage open IoT systems.[190] Such nudging of the industry in the direction of greater

183. *See id.* at 3.
184. *See id.* at 21–24.
185. *Id.* at 22.
186. *Id.* at 23.
187. *Id.*
188. *Id.* at 24.
189. *Id.*
190. Walport, *supra* note 50, at 7.

interoperability can be helpful. However, mandating interoperability in every segment of the IoT market is bound to be counterproductive. First, such mandate is unlikely to be technology-neutral, prematurely favoring one emerging technology over another. Second, joint industry efforts such as one led by oneM2M can broaden adoption of common solutions (including privacy and security standards) across industrial sectors and countries. This will lead to greater interoperability than having multiple jurisdictions impose various IoT regulations. Finally, as some economists have pointed out, despite efficiency gains from network effects in having one system, the existence of two or more competing systems can promote product variety and innovation, and thus, be more desirable.[191] One needs to only consider the competition between iOS and Android to appreciate the resultant speed of innovation in the smartphone OS market. Thus, governments can incentivize industry to move to open systems, but would be well advised to refrain from prematurely mandating broad standards.

191. Michael Katz & Carl Shapiro, *Systems Competition and Network Effects*, 8 J. ECON. PERSPECTIVES 2, 95 (1994).