UIC John Marshall Journal of Information Technology & Privacy Law

Volume 32 | Issue 4 Article 2

Spring 2016

Smart Washers May Clean Your Clothes, But Hacks Can Clean Out Your Privacy, and Underdeveloped Regulations Could Leave You Hanging on a Line, 32 J. Marshall J. Info. Tech. & Privacy L. 259 (2016)

Nikole Davenport

SMART WASHERS MAY CLEAN YOUR CLOTHES, BUT HACKS CAN CLEAN OUT YOUR PRIVACY, AND UNDERDEVELOPED REGULATIONS COULD LEAVE YOU HANGING ON A LINE

NIKOLE DAVENPORT

ABSTRACT:

A house is equipped with a smart clothes washer, an intelligent HVAC system and a video enabled home security system, all running through the home network - it reduces the noise by doing laundry when no one is at home, saves energy costs by automatically changing the temperature depending who is in a room, lets the owner remotely see the kids walk in the door after school, and keeps the house safe - the owner is maximizing the use of the Internet of Things ("IoT") devices (i.e. a network of everyday objects connected to the Internet and to each other). However, the home owner has also created at least four points for data vulnerabilities, giving a hacker four opportunities to enter the home. A single hack can allow a wrongdoer to determine when no one is home and access an empty house, spy on the children and collect PIN numbers and any sensitive data recorded by any or all of the IoT service providers, like credit card numbers. When such a data breach happens, what legal protections does a consumer have? What regulatory infrastructure is in place to prevent this type of intrusion, what data is considered protectable personal identifying information (PII), what obligations do the manufacturers have to prevent hacks, and what remedies are available to those whose privacy has been corrupted? This paper attempts to address the growing infiltration of the IoT into everyday life and to answer some of these questions by looking at the current US legal framework addressing privacy.

INTRODUCTION

The Internet of Things ("IoT") is a term referred to in the media on a daily basis, with experts portending that integrated technology will improve the quality of life for all. However, little is published regarding the mechanics of how the IoT will become incorporated into everyday living, the potential risks

raised by adoption, or how users may be protected when the data collected by the IoT is breached. IoT technology is accelerating at warp speed, while the law regulating the data it generates is slowly evolving, thereby creating a gap that continues to grow. Lengthy and comprehensive scholarship regarding the legal implications of IoT adoption is scarce, based largely on the fact that technological advancements are surpassing the parameters of Moore's Law.

To date, the most comprehensive legal assessment of the IoT and privacy focused on a number of IoT devices in the marketplace, addressing primarily sensor fusion, de-identification shortcomings, the potential legal discrimination that might occur due to non-financial data collected by IoT devices, and the gaps in the law that leave consumers vulnerable.[1] Privacy and safety concerns regarding wearable IoT devices have been explored in the legal context in an article that considered the appropriateness of government regulation at the infancy of the technology. [2] The authors concluded that even though the challenges are considerable, "it is essential that experimentation and innovation in this space not be derailed on the basis of speculation about hypothetical worst-case scenarios."[3] Further, issues related to security and machine to machine interaction have been assessed, but merely point to the fact that this is just the beginning of the process in attacking IoT device privacy without drawing conclusions.[4] Various other short articles and legal blogs have addressed IoT technology and privacy from broad overviews,[5] to narrow issues,[6] without arriving at firm assessments or recommendations. Legal studies have

---

1. Scott R. Peppet, *Regulating the Internet of Things: First Steps Towards Managing Discrimination, Privacy, Security & Consent*, 93 TEX. L. REV. 85, (2014).

2. Adam D. Thierer, *The Internet of Things and Wearable Technology: Addressing Privacy and Security Concerns without Derailing Innovation*, 21 RICH. J. L. & TECH. 6 (2015), http://jolt.richmond.edu/v21i2/article6.pdf.

3. Thierer, *supra* note 2 at 117.

4. Eric Barbry, *The Internet of Things, Legal Aspects What Will Change (Everything)…*, COMMUNICATIONS & STRATEGIES, No. 87 3rd Q. 2012 at p. 87; *see also* Sarah McMahon, Comment, *Internet of Things: A Privacy Law Case Study*, STUDENT WORKS (April 1, 2015), http://digitalcommons.law.uga.edu/cgi/viewcontent.cgi?article=1000&context=stu_papers; Rolf H. Weber, *Internet of Things – New Security and Privacy Challenges*, 26 COMPUTER L. & SECURITY REV. 23,23-30 (2010).

5. *See* Chris Folk, Dan C. Hurley, Wesley K. Kaplow, & James F.X. Payne, *The Security Implications of the Internet of Things*, AFCEA INTERNATIONAL CYBER COMMITTEE 1, 10 (Feb. 2015), http://www.afcea.org/committees/cyber/documents/InternetofThingsFINAL.pdf; *see also* THOMAS COOLEY, LAW OF TORTS (2nd ed., Vol. 29, 1888); *see also* Lauren Henry Scholz, *Information Privacy and Data Security,* CARDOZO L. REV. DE NOVO 107-118 (2015); *see also* Barbry, *supra* note 4, at 87.

6. Barbara Murphy Melby & Christopher C. Archer, *The Internet of Things (Part 1): A Brief Introduction for Lawyers*, THE NATIONAL LAW REVIEW (Nov. 18, 2014); H. Michael O'Brien, *The Internet of Things and the Inevitable Collision with Product Liability PART 4: Government Oversight,* THE NATIONAL LAW REVIEW (Oct. 17, 2015); Eilene Spear, *Data Privacy and Data Security: Two Sides of the Same Coin A Conversation with Patrick Manzo, Executive Vice President, Global Customer Service and Chief Privacy Officer of Monster Worldwide, Inc*., NATIONAL LAW REVIEW (May 11, 2015); Manoj Khandekar, *In with the New: Expect FTC Activity on IoT in 2015,* THE NATIONAL LAW JOURNAL (Jan. 26, 2015); Omer Tene, *People Like You,* YALE J. OF L. & TECH. Blog (Nov. 18, 2015), http://yjolt.org/blog/2015/11/28/people-you.

investigated privacy as it relates generally to technology, but without a specific focus on the IoT.[7] The primary focus, as discussed herein, was on the technological and privacy concepts regarding the IoT generated by the industry itself, tech periodicals, and the Federal Trade Commission.[8]

This article intends to provide a more comprehensive overview regarding how the IoT technology will advance from a series of novel products to more robust integration into daily life, while raising the privacy issues that are emerging by the use of the IoT. This article will also study the disparate series of laws and regulations created under the sectoral model (i.e. laws which are industry specific and not global) employed in the United States. It will provide an overview of the data privacy laws in the US on multiple tracks – federal legislation, regulatory agency rules and enforcement, state legislation with Attorneys General ("AG") activism, and in the courts through class actions – and assess the results of the government's reliance on industry self-regulation, as of June 2016. As discussed in this paper, although there is a plethora of different laws, regulations, proposals, and standards that might protect IoT consumers, there are more gaps than coverage for users, and there is more work needed to minimize the risks that come along with the convenience of using the IoT devices.

I. THE INTERNET OF THINGS

The "Internet of Things" (the "IoT") refers to the ability of one device to connect to other devices through wireless data infrastructure.[9] It links physical objects embedded with sensors and actuators to the Internet to allow them to exchange data, and communicate with each other.[10] McKinsey Global Institute, a research institute created to address the evolving global economy, describes the IoT in more detail, defining it as "[L]inking machinery, equipment and other physical assets with networked sensors and actuators to capture data and manage performance, enabling machines to collaborate and even act on new information independently."[11]

It is anticipated that the conveniences and efficiencies offered by the IoT

---

7. Jules Polonetsky & Omer Tene, *Privacy and Big Data: Making Ends Meet*, 66 STAN. L. REV.25 (Sept. 3, 2013) (weighs privacy risks against big data rewards); Scholz, , *supra* at note 5 (assesses the history of privacy laws and looks at the application to the separate, but entwined, issues of information privacy and data security).

8. Julie Brill, *The Internet of Things: Building Trust and Maximizing Benefits Through Consumer Control*, 83 FORDHAM L. REV. XX, 209 (2014).

9. Electronic Privacy Information Center, *Internet of Things (IoT),* https://epic.org/privacy/internet/iot/ (last visited Dec. 8, 2015).

10. *SIGFOX Partners With San Francisco to Connect the City to SIGFOX's Internet of Things Network*, M2MWORLDNEWS.COM (Oct. 29, 2015), http://m2mworldnews.com/2015/10/29/62009-sigfox-partners-with-san-francisco-to-connect-the-city-to-sigfoxs-internet-of-things-network/.

11. Melby & Archer, *supra* note 6; GLOBAL INSTITUTE, http://www.mckinsey.com/insights/mgi/about_us (last visited Dec. 11, 2015).

will improve our quality of life and reduce energy consumption. Within the next ten years, industry experts expect that IoT devices will become more pervasive than mobile phones.[12] The anticipated ubiquity is because every manufactured thing will have chips embedded in them to report data and provide interconnectivity. General Electric has plans to put chips "into everything that spins," from consumer light bulbs to industrial engines.[13]

The interconnected world is already integrated into society, from Fitbit devices to remotely operated home camera systems, people rely on connected insulin pumps, and are obsessed with their "smart" televisions. Moreover, different everyday devices, such as GPS navigation systems and e-book readers already connect to the Internet. The reach of the IoT is endless, encompassing personal health (watches that record heart rate, movement and sleeping patterns, and scales that log weight records), household appliances (smart refrigerators and dryers), security systems, black boxes in cars, and even drones.

A current example of IoT technology is the integration of Google's Nest with Whirlpool's new home washers and dryers which enabled the dryers to time their cycles based on data from the Nest thermostat regarding whether the consumer is home.[14] In the future, the IoT may allow a smoke detector to send a text when the alarm is activated or when it has a low battery; a device might include a tracker to locate a stolen bicycle, and, in the public sector, a sensor placed on a fire hydrant could alert authorities about leaks.[15] The vision for the IoT includes connected utility meters, automotive connectivity (autonomous vehicles, fleet management, real time traffic information to vehicles, security monitoring and reporting), and medical alerting.[16] The types of applications – ranging from agriculture, connected health, security, and logistics – that may benefit from the IoT is limitless."[17]

The IoT is a broad concept used colloquially to encompass many or all of the interconnected devices in our future. But industry experts identify three subsets to the general IoT category which are the Industrial Internet (i.e. all interconnected products, sensors, controls, etc., used in industry and busi-

---

12. *Internet of Things Research Study,* HEWLETT PACKARD ENTERPRISE (2015), http://www8.hp.com/h20195/V2/GetPDF.aspx/4AA5-4759ENW.pdf.

13. Jon Gertner, *Behind GE's Vision For The Industrial Internet Of Things*, FAST COMPANY (June 18, 2014); Dimitri T. Saad & Carmen Oveissi Field, Deloitte Advisory, Luncheon Presentation at the Institute of Continuing Legal Education Georgia: Internet of Things – Legal and Compliance Considerations, (Oct. 23, 2015).

14. Folk, Hurley, Kaplow & Payne, *supra* note 5.

As addressed further below, the convenience and energy saving benefits of this technology will need to be balanced against privacy and safety issues. With this particular technology, both Google *and* Whirlpool know the consumer is not home, thereby doubling the cyber threat and physical risks the consumer faces.

15. *SIGFOX Partners with San Francisco*, *supra* note 10.

16. Futureworks *LTE-M Optimizing LTE for the Internet of Things*, NOKIA NETWORKS (2015), http://networks.nokia.com/sites/default/files/document/nokia_lte-m_-_optimizing_lte_for_the_internet_of_things_white_paper.pdf.

17. *SIGFOX Partners with San Francisco, supra* note 10.

ness), the Internet-of-everything (consumer objects and systems that combine people and data), and the Cyber physical systems (which are the systems that connect it all).[18] Each subset may face individual issues with implementation, regulation, and assimilation. However, for the purposes of this paper, the IoT is referenced broadly and addresses the IoT in its most inclusive form.

II. VOLUME AND SCALE

The estimates surrounding the volume of devices and economic impact of the IoT focus mainly on the year 2020, a scant four years away. Shorter term predictions made in 2014 suggested that there would be 3.9 to 25 billion connected devices at the end of 2015,[19] however, the actual number of devices currently employed is closer to 1 billion.[20] Consistent with these drastic discrepancies, expert estimates regarding the number of IoT devices that will be integrated into society in 2020 vary from 20 billion[21] to 50 billion, and eventually 200 billion.[22] Approximations as to the economic value created by the IoT in 2020 are equally staggering and range from $3.9[23] trillion to $19 trillion.[24] However, Beecham Research, an international organization leading research and analysis in IoT market development, is warning companies "not to

18. Folk, Hurley, Kaplow, & Payne, *supra* note 5.

19. Colin Barker, *25 Billion Connected Devices by 2020 to Build the Internet of Things*, ZDNET.COM (Nov. 11, 2014), http://www.zdnet.com/article/25-billion-connected-devices-by-2020-to-build-the-internet-of-things/; Gil Press, *Internet of Things by the Numbers: Market Estimates and Forecasts,* FORBES/TECH (Aug. 22, 2014) http://www.forbes.com/sites/gilpress/2014/08/22/internet-of-things-by-the-numbers-market-estimates-and-forecasts/.

20. *State of the Market THE INTERNET OF THINGS 2015 Discover How IoT is Transforming Business Results,* VERIZON (Feb. 2015), http://www.verizonenterprise.com/resources/reports/rp_state-of-market-the-market-the-internet-of-things-2015_en_xg.pdf. The Organization for Economic Co-operation and Development (OECD) compiled data detailing Internet connected devices by country in 2015 which shows just seven countries with interconnected devices at a rate higher than 20 units per 100 people, http://dx.doi.org/10.1787/888933225312.

21. Barker, supra note 19; Nathan Eddy, *IoT Devices to Almost Triple by 2020, to 38 Billion*, EWEEK.COM (July 31, 2015), http://www.eweek.com/small-business/iot-devices-to-almost-triple-by-2020-to-38-billion.html; Gulio Coraggio, *Fear Cannot Stop the Internet of Things*, DLA PIPER IPT ITALY BLOG (Aug. 6, 2015), http://blogs.dlapiper.com/iptitaly/?p=57173.

22. Julie Brill, *The FTC and the Future of Privacy and Data Security*, , (Sept. 15, 2015), *available at* https://www.ftc.gov/system/files/documents/public_statements/804391/150924berkeleybcltremarks_.pdf.

23. James Manyka, Michael Chui, Peter Bisson, Jonathan Woetzel, Richard Dobbs, Jacques Bughin & Dan Aharon, *The Internet of Things: Mapping the Value Beyond the Hype*, MCKINSEY GLOBAL INSTITUTE (June 2015), 36, http://www.mckinsey.com/insights/business_technology/the_internet_of_things_the_value_of_digitizing_the_physical_world. McKinsey Global Institute estimates IoT impact will be between $3.9 and $11.1 trillion annually by 2025.

24. Press, *supra* note 19 ($19 trillion in economic value created by the IoT in 2020); Saad & Field, *supra* note 13 (Deloitte estimates $9 trillion by 2020).

believe all the hype and over optimistic predictions."[25] Robin Duke-Woolley, CEO at Beecham Research, cautions, "[W]hile some households may have a dozen or more connected devices there is no evidence yet of connected devices in the home taking off in a big way."[26]

Regardless of the inconsistency with future assessments, the "big way" will eventually come as devices proliferate and the infrastructure expands. Industry executives and academics have various theories regarding the causes of the current explosion in IoT products.[27] While "Moore's Law" is relevant, and there have been substantial decreases in prices for sensors, processors and networking, a more practical reason for the growth may be that four of the largest network providers, Amazon, Cisco, GE and IBM, have committed to IoT, with network modifications that will simplify processes and reduce the costs for network connectivity.[28] Such investments are economically based in both the growth of sales for products and services, as well as in the increased productivity and lower costs that will result from the gross implementation of the IoT into personal and industrial uses.

For instance, energy companies have adopted industrial IoT technologies to optimize resources, assets, and performance incrementally, which resulted in increases in profitability.[29] Access to extensive data in real time, as generated by the IoT, creates significant opportunities for companies to reduce downtime and improve processes by addressing problems and abnormalities before they lead to crises, while creating safer environments and preventing incidents.[30] The opportunities to drive better performance are not limited to resource productivity and increased safety, they also offer consumer knowledge. By installing and connecting sensors, companies can obtain better insight into their customers by monitoring how they use their products as they actually engage, and harvest that information for their own business purposes. Such data acquisition will allow IoT providers, and those who analyze the data it produces, to identify and drive improvements in performance and value, and will permit prompt action with respect to difficulties that cus-

---

25. Robin Duke-Wooley, *Beecham Research Urges Industry to 'Get Real' About IoT Predictions,* REALWIRE (Nov. 5, 2015), http://www.realwire.com/releases/Beecham-Research-urges-industry-to-get-real-about-IoT-predictions.

26. *Id*.

27. *Id.*; Press, *supra* note 19; *Dave Sobel, Can You Handel the IOT Explosion? THE VAR GUY BLOG (Nov. 10, 2015)* http://thevarguy.com/blog/can-you-handle-iot-explosion.

28. Press, *supra* note 19 (memorializing interview of Janus Bryzek, VP at Fairchild Semiconductor and "the father of sensors").

29. Trey Thoelcke, The *Internet of Things Will Provide Top Companies Huge Opportunity*, YAHOO FINANCE (Jan. 8, 2014) http://finance.yahoo.com/news/internet-things-top-companies-huge-151545735.html; Leo Sun, *How Amazon.com Inc. Plans to Profit from the Internet of Things,* THE MOTLEY FOOL (Oct. 14, 2015), http://www.fool.com/investing/general/2015/10/14/how-amazoncom-inc-plans-to-profit-from-the-interne.aspx.

30. Jane Collis, *Internet of Things: Generating Opportunity Behind the Buzz Words in the Energy Sector*, DLA PIPER LLP CLIENT ALERT (Nov. 3, 2015), http://www.lexology.com/library/detail.aspx?g=0675dcaf-a0b4-4133-8e94-05ca96477362.

tomers experience.[31]

III. HOW THE IOT WORKS

A. Integration Explanation

It is easy to see IoT devices, like the Fitbit on your wrist, but the network that will allow the Fitbit to connect the data it produces seamlessly to complimentary devices is invisible. In fact, the future state of the infrastructure for transferring the data is still not certain, which may explain why the estimates of billions and trillions of devices within the next four years will not become a reality. This is simply because the connectivity platforms are not yet ready to handle the data.

The IoT continuum starts with smart IoT devices, which provide access to information and data. It progresses through mobility sources and gateway connectivity, then to a cloud for storage. [32] From there it is accessible for analytics - integration, aggregation, assimilation, and/or utilization. When firmly established, it is envisioned that IoT networks within the home, factory, or other setting, will find a local gateway or 'hub' that is connected through a local network to the devices near the hub. It will then process and pass data from the IoT devices to a cloud computing platform.[33] The devices will direct the parameters for processing the data, but the data itself will be stored in a cloud, awaiting the next command, or lingering for use by anyone with access to it. In this process, the remote cloud computing platforms are as important, or more, than the device itself, to any IoT system.[34] The basis for IoT data advancement is this connectivity process, that is, it relies on technology working to create full eco-systems for data to connect with each other seamlessly. The network of sensors, radiofrequency chips, and storage are the backbone of the technology.[35]

B.Network Implementation

The IoT needs machine-to-machine communication (i.e. data communication among devices without human interaction), to advance.[36] One of the reasons that the IoT may not hit the 2020 estimates of devices and economic value is the current lack of connectivity. However, with many companies pursuing different alternatives to addressing the shortfall, the short-coming will be short-lived. Beecham Research points "to new low power, low data

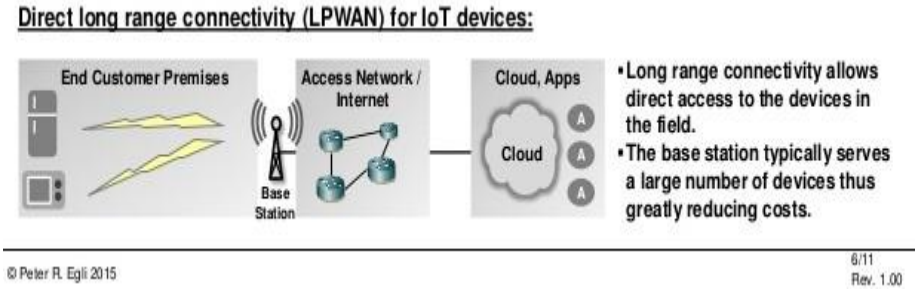
---

31. *Id*.
32. Robert S. Berezin, *The Next Big Thing: 'Internet of Things' Litigation and Regulatory Risk*. NEW YORK LAW JOURNAL, (Nov. 2, 2015).
33. *Id*.
34. *Id*.
35. Barbry, *supra* note 4, at 87.
36. *LTE-M Optimizing*, NOKIA NETWORKS *supra* note 16.

rate, long range network technologies such as Low Power Wide Area Networks (LPWANs)[37] to provide a growth spurt to the IoT market."[38] Nokia asserts that fixed and short range communications as well as a significant number (an estimated seven billion by 2025) of connections via cellular IoT and LPWANS will address most of the connection deficiencies.[39] Duke-Woolley of Beecham Research further contends that the new cellular technology becoming available within the next two years, termed LTE-M or Narrowband IoT, derived from 4G technology, will provide the real growth momentum for the low data rate applications of the IoT.[40]

The joint support of Ericsson AB, Intel Corp. and Nokia Corp for a new specification called Narrow-Band Long-Term Evolution (NB-LTE) may further fuel the explosion. The three had previously joined with AT&T, Sprint, and Verizon Wireless in August 2015 to propose a way to use as much existing LTE technology as possible for IoT technology. "NB-LTE technology allows a high re-use of already existing LTE network technology for both infrastructure and chipset that will permit a fast adoption and maximize economies of

37. LPWAN is wireless network technology specialized for interconnecting devices with low-bandwidth connectivity. LPWAN have longer range, lower costs and decreased power requirements, compared to mobile networks, are thought to enable a much wider range of machine-to-machine (M2M) and IoT applications. TECHTARGET IOT AGENDA, http://internetofthingsagenda.techtarget.com/definition/LPWAN-low-power-wide-area-network (Last visited Feb. 4, 2016). *See also*, Peter R. Egli, *LPWAN Technologies for Internet of Things (IoT) and M2M Scenarios* (Mar. 13, 2015), http://www.slideshare.net/PeterREgli/lpwan. Image taken from http://www.slideshare.net/PeterREgli/lpwan.



38. Duke-Wooley, *supra* note 25.

39. *LTE-M Optimizing*, NOKIA NETWORKS *supra* note 16. Further, the international mobile broadband association GSMA announced the establishment of a mobile IoT initiative in August 2015, confirming that LPWAN solutions are likely to fulfill the full potential of IoT; GSMA Press Release, *GSMA Launches Low Power Wide Area Network Initiative to Accelerate Growth of the Internet of Things* (Aug. 20, 2015), http://www.gsma.com/newsroom/press-release/gsma-launches-low-power-wide-area-network-initiative-accelerate-growth-internet-of-things/;

To this end, "26 of the world's leading mobile operators, along with infrastructure manufacturers, OEMs, module and chipsets vendors, are lending support to this initiative to accelerate development of LPWA solutions in licensed spectrum." Steve Bell, *Narrowband Cellular IoT Offers Clean Slate*, LIGHTREADING NETWORKING THE COMMUNICATIONS INDUSTRY, http://www.lightreading.com/iot/narrowband-cellular-iot-offers-clean-slate/a/d-id/717987.

40. Duke-Wooley, *supra* note 25.

scale."[41] Similarly, yet with a slightly different methodology, others are endorsing using Narrowband Cellular IoT (CIoT) as a new platform for interconnectivity. Narrowband, however, also relies on the existing 4G and 4G LTE networks to support the anticipated tsunami of IoT connected devices. [42] Others offer competing "clean slate" proposals that require dedicated investments for network infrastructure and chipsets, as well as the creation of a new ecosystem which may take more time to develop.[43]

Beating the others to the market, SigFox is currently connecting San Francisco for the IoT using discarded cordless phone technology. It was recently announced that SigFox, self-described as "the first and only company providing global cellular connectivity for the Internet of Things, fully dedicated to low-throughput communications,"[44] is providing San Francisco with "a dedicated Internet of Things network that will provide low-cost, energy-efficient and two-way connectivity for smart-city programs."[45] SigFox's network will rely on the unlicensed 915-megahertz spectrum band commonly used by cordless phones. Albeit, objects connected to this network are only able to operate at very low power, (just 100 bits per second transmissions — 1,000 times slower than the smartphones), that may be enough for IoT applications.[46]

Yet another theory about why the IoT connectivity may expand exponentially in the near future focuses on the roll out of IPv6 IP internet addresses. The AFCEA and sensor expert Janus Bryzek believe that the expansive changes to the IP addresses is expected to increase the number of smart connected devices 50 billion."[47] Regardless of which technical method of network connectivity prevails, the race to supply the market is in full swing, and with it, the proliferation and integration of IoT devices.

---

41. Sead Fadilpašić, *Intel, Nokia and Ericcson support a new Iot standard*, ITPROPORTAL.COM (Feb. 11, 2015) http://www.itproportal.com/2015/11/02/intel-nokia-and-ericcson-support-a-new-iot-standard/.

42. Dan Jones, *Ericsson, Intel, Nokia Back New Narrowband LTE IoT Spec.*, LIGHT READING, Networking the Communications Industry (Sept. 11, 2015), http://www.lightreading.com/mobile/4g-lte/ericsson-intel-nokia-back-new-narrowband-lte-iot-spec-/d/d-id/718162.

43. Some experts believe that "After years of convergence toward a single technology -- LTE -- the industry is recognizing that, in order to be able to serve the diverse but relatively simple connectivity and data requirements of the machine-to-machine (M2M) and IoT markets, a single technology may not be capable of delivering on all use cases. Consequently, the GSMA identified that its initiative will focus on three complementary licensed 3GPP standards: LTE evolutions, GSM evolutions and clean-slate technologies." Bell, *supra* note 37.

44. SIGFOX, www.sigfox.com (last visited Dec. 8, 2015).

45. *SIGFOX Partners with San Francisco, supra* note 10.

46. Tom Simonite, *Silicon Valley to Get a Cellular Network, Just for Things*, MIT TECH. REV. (May 20, 2014), http://www.technologyreview.com/news/527376/silicon-valley-to-get-a-cellular-network-just-for-things/.

47. Folk, Hurley, Kaplow, & Payne, *supra* note 4, at 4. Gil Press, *The Internet of Things: Why Now and How Big?* THOUGHT LEADERSHIP MARKETING BLOG (Sept. 2, 2014), https://www.linkedin.com/pulse/20140902175847-3639577-the-internet-of-things-why-now-and-how-big.

IV. BIG DATA & EVERYDAY LIFE

Once transmitted and amassed, the volume of IoT data is expected to create powerful data sets from which companies can derive valuable insights.[48] The creation of the expansive data sets can be explained using the computer science phenomenon of sensor fusion which "dictates that the information from two disconnected sensing devices can, when combined, create greater information than that of either device in isolation."[49] It is a common sense theory, borne out by science, that the combining of sensor data from different sources will create a resulting set of information that is better than the disparate information from each individual source.[50] The technical problem that arises from this is that sensor data can combine in unexpected ways, "giving rise to powerful inferences from seemingly innocuous data sources."[51]

The use of multiple IoT devices will provide consumers with practical benefits by allowing providers to facilitate communication with consumers through the collection and transmittal of data, a byproduct of which is the provider's ability to compile large amounts of data for itself and for third parties.[52] Consumer convenience, however, accompanies the side effect that personal information regarding our bodies, lifestyles, geolocations, and activities within and outside our homes will be accessible and easily available to third parties. When combined with other online and offline data, which is a goal of data miners, the new data sources produced by the IoT have the potential to create alarmingly detailed and personal consumer profiles.[53] Processing the aggregated data obtained through IoT devices will ultimately form a 'Big Data' repository to access and use.[54]

This process is already occurring. ONZO, a company that focuses on energy consumption and consumer behavior to provide forecasting to utilities customers, operates with the stated goal of providing "unprecedented insights" into how, when and where consumers use energy using big data.[55] ONZO describes its process as "leveraging granular smart meter data" using "patented algorithms" to "result in richer, highly accurate, customer-specific insights that help utilities improve customer engagement and energy efficiency, while reducing churn and creating new revenue opportunities."[56] In advertising its functions, ONZO states, "Complex big data is a goldmine of information; how-

48. Berezin, *supra* note 32.
49. Scott R. Peppet, *supra* note 1, at 7.
50. *Id.* at 31.
51. *Id.* at 29.
52. Melby & Archer, *supra* note 4.
53. Brill, *supra* note 8, at 209.
54. Berezin, *supra* note 32 (which provides in relevant part that: "In this sense, the IoT is a classic application of 'Big Data'").
55. *ONZO Announces New Release of Consumer Engagement and Insight Platform*, ONZO.COM (Sept. 7, 2015) http://www.onzo.com/onzo-announces-new-release-of-consumer-engagement-and-insight-platform/.
56. *Id.*

ever, expertise is needed to analyze this data for insight that benefits both energy providers and their consumers."[57]

A.Data Analytics

As described above, the IoT is interrelated with "Big Data," but to understand the potential downsides, it is important to know what that means and how it is applied.[58] Unfortunately, there is not a universal answer to the definition of Big Data, as it depends on to whom you ask the question. A generic answer, provided by data scientist John Rauser, is that "big data" is simply "any amount of data that's too big to be handled by one computer."[59] The reality of Big Data is that it is a treasure-trove for the field of data analytics – useful to improve efficiency, service, safety and more – but it also exposes consumers to a variety of risks.

Data brokers, those who deal in data analytics, according to the Federal Trade Commission ("FTC"), are entities that most people do not know anything about because they do not interact with consumers. Rather, they work behind the scenes, gathering profiles from vast amounts of online and offline data. The data growth that will come because of the IoT will only increase their importance to companies and marketers going forward. As the FTC's recent report on data brokers details, these profiles may reveal where consumers live, how much they earn, their race, health conditions, and interests."[60] These distinctions were addressed specifically in the FTC Data Brokers: A Call for Transparency and Accountability report that details how vast amounts of data can be culled to create alarmingly detailed consumer profiles.[61] Examples include groups consisting of consumers categorized as "Financially Challenged," or "Bible Lifestyle," or "Diabetes Interest."[62] Given that data brokers are able to create profiles with this level of specificity based on 2014 technology, one can assume that profiles created using IoT data in 2020 will be significantly more detailed and specific. In its 2015 report regarding the IoT, Inter-

57. ONZO, http://www.onzo.com/about-us/ (last visited Dec. 10, 2015); Louise Downing, *Onzo Study Harvesting Smart-Meter Data,* BLOOMBERG (May 12, 2014), http://www.bloomberg.com/news/articles/2014-05-11/wpp-unit-onzo-study-harvesting-smart-meter-data.

58. EXECUTIVE OFFICE OF THE PRESIDENT, *Big Data: Seizing Opportunities, Preserving Values* (May 2014) at p. 3, https://www.whitehouse.gov/sites/default/files/docs/big_data_privacy_report_may_1_2014.pdf. (Which provides in relevant part that: "Big data may be viewed as property, as a public resource, or as an expression of individual identity,").

59. Brandon Butler, *Defining 'Big Data' Depends on Who's Doing the Defining*, NETWORK WORLD (May 10, 2012), http://www.networkworld.com/article/2188435/data-center/defining--big-data--depends-on-who-s-doing-the-defining.html.

60. Brill, *supra* note 8, at 12 n. 52,13 n. 57.

61. Federal Trade Commission, *Data Brokers: A Call for Transparency and Accountability*, (2014) https://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf.

62. *Id*.

net of Things, Privacy and Security in a Connected World, the FTC contends that the rush is on for companies to maximize use of IoT data collected in someone's personal and private space.[63] Most recently, in January 2016, the FTC issued yet another report on big data, warning businesses to "ensure that their big data use does not lead to harmful exclusion or discrimination."[64]

B.Individual Impact

IoT technology will create an infinite number of data points about each user, and while providing significant benefits, it will provide those who view the data absolute transparency about each person. Societal adjustments to this type of transparency may take time. When more fully implemented, the IoT may change personal interactions to the extent that our personally curated world may contradict our actual world.[65] In the world now, we present a self-curated presentation of ourselves by controlling the online data we disseminate (our social media mainly, but also professional work biographies and records of organizational support); in the world where IoT information is pervasive and integrated, we are merely the data points that are collected about us. We might tell the DMV that we weigh 120 pounds, while our Fitbit registers us at 150, a fact seamlessly transmitted to the DMV clerk through wireless interconnectivity. We may post only photos of ourselves at the gym and at fancy restaurants, while our IoT data shows that we exercise less than once a month and eat fast food five times a week - information easily transferred to our health insurer or doctor. In a connected IoT world, one no longer needs to self-report, rather there may be digital data exchanges based solely on verifiable facts that may work to our detriment.

V. POTENTIAL HARMS

Regulators and industry professionals recognize that as the number of connected IoT devices increases, security concerns multiply exponentially. It is widely perceived that companies will have access to the most sensitive personal data about people, including social security numbers and banking in-

63. Federal Trade Commission, *Internet of Things, Privacy and Security in a Connected World*, FTC STAFF REPORT (Jan. 2015) at p. 17, https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf.

64. FTC Press Release, *FTC Report Provides Recommendations to Business on Growing Use of Big Data*, FEDERAL TRADE COMMISSION (Jan. 6, 2016), https://www.ftc.gov/news-events/press-releases/2016/01/ftc-report-provides-recommendations-business-growing-use-big-data; Federal Trade Commission, *Big Data: A Tool for Inclusion or Exclusion? Understanding the Issues,* FTC STAFF REPORT (Jan. 2016), https://www.ftc.gov/system/files/documents/reports/big-data-tool-inclusion-or-exclusion-understanding-issues/160106big-data-rpt.pdf.

65. Cindy A. Liebes, Presentation at the Institute of Continuing Legal Education Georgia: *FTC Trade Commission: Privacy, Security and a Guide for Business* presentation during the *Internet of Things – Legal and Compliance Considerations* (Oct. 23, 2015).

formation, and that maintaining data responsibility requires taking appropriate steps.[66]

A.Cybersecurity & Data Privacy

Privacy of personal information and data security speak to the same concerns and, from the consumer perspective, impact identical issues of trust and legitimacy.[67] They have been described as two sides of the same coin[68] and while data privacy and data security are often used interchangeably, it is important to realize the difference, both in practice and in legal implication. Data privacy relates to the person whose confidential information must be kept safe. Data security is the mechanism for keeping it safe. Data security implicates the computer hardware – firewalls, antivirus software, encryption, and security measures – data security operates as shield to keep unauthorized parties from stealing a person's confidential information.[69]

The potential for harm related to data privacy and security breaches is present and concrete. On September 10, 2015, the Federal Bureau of Investigation ("FBI") issued a public service announcement describing IoT cybercrime risks, providing details of how IoT cybercrime might impact individuals, and suggesting protective measures.[70] To warn the public of potential risks related to the IoT, the FBI stated:

As more businesses and homeowners use web-connected devices to enhance company efficiency or lifestyle conveniences, their connection to the Internet also increases the target space for malicious cyber actors. Similar to other computing devices, like computers or Smartphones, IoT devices also pose security risks to consumers. The FBI is warning companies and the general public to be aware of IoT vulnerabilities cybercriminals could exploit, and offers some tips on mitigating those cyber threats.[71]

According to the Identity Theft Resource Center, over the past ten years there have been over 5,600 data security breaches, impacting nearly a billion

66. HEWLETT PACKARD, *supra* note 12.

67. Scholz, *supra* note 5, at 113.

68. Patrick Manzo, Executive Vice President, Global Customer Service and Chief Privacy Officer of Monster Worldwide, Inc., says, "Data security and data privacy are two sides of the same coin, and we trade that coin for consumer trust." He "defines data security as, simply, knowing where your data is located, and who may access the data. Data privacy is predicated on data security and requires further understanding how personal data is being collected, processed (and by whom), and transferred, and the consistency of these practices with applicable laws, regulations, and the reasonable expectations of the relevant consumers." Eilene Spear, *supra* note 5.

69. Diane D. Reynolds, *Privacy vs. Security – Privacy and Data Security Insight*, UPDATES AND ANALYSIS FROM TAFT PRIVACY AND DATA SECURITY ATTORNEYS (Nov. 10, 2015), http://www.privacyanddatasecurityinsight.com/2015/11/privacy-vs-security/.

70. Federal Bureau of Investigation, *Internet of Things Poses Opportunities for Cyber Crime*, (Sept. 10, 2015), http://www.ic3.gov/media/2015/150910.aspx.

71. *Id*.

records.[72] Six hundred and ninety of those breaches occurred in the first 11 months of 2015 alone, thereby highlighting the reality of cyber security threats.[73] Any IoT device is only as secure as the weakest link in the network it communicates with, creating risks at each level of the IoT continuum, from the device, Wi-Fi connections, mobile operating systems, to the cloud and potentially third-party devices.[74] Thus, the number of security breaches will most likely increase substantially when the estimated billions of IoT devices are employed in 2020 and beyond.

With respect to IoT specific cybersecurity weaknesses, the Open Web Application Security Project (OWASP) Internet of Things Project identified a top 10 list of IoT vulnerabilities 2014.[75] The top concerns include:

> 1. Username Enumeration – ability to collect a set of valid usernames by interacting with the authentication mechanism;
>
> 2. Weak Passwords – ability to set account passwords to '1234" for example; and,
>
> 3. Unencrypted Services – network services not properly encrypted to prevent eavesdropping by attackers, or, if they are encrypted, it is poorly and improperly implemented.[76]

These risks were borne out in a study conducted by Hewlett Packard[77] which analyzed ten IoT devices from manufacturers of smart TVs, webcams, home thermostats, door locks, alarms and scales, and found alarming shortfalls in data security, nearly mirroring with OWASP concerns, including:

> 70% of devices, along with their cloud and mobile application, enable an attacker to identify valid user accounts through account enumeration;
>
> 80% failed to require sufficiently complex passwords; and
>
> 70% used unencrypted network service.[78]

---

72. IDENTITY THEFT RESOURCE CENTER, http://www.idtheftcenter.org/id-theft/data-breaches.html (last visited Dec. 5, 2015).

73. Chelsey Levingston, *The Biggest Data Breaches to Date in 2015*, DAYTON DAILY NEWS (Nov. 30, 2015) http://www.daytondailynews.com/news/news/the-biggest-data-breaches-to-date-in-2015/npYrw/; The five largest breaches of 2015 have been identified, three of which are by health insurers - #1s Anthem Inc. (78.9 million commercial health records), Premera Blue Cross (11 million) and Excellus Blue Cross (10 million), the second largest breach was by the United States Office of Personnel Management (over 25 million background records, including social security numbers, in two different hacks) and, third was T-Mobile/Experian (15 million credit records with complete PI).

74. Benjamin Kleine, Bethano Lobo & Amanda Levendowski, *Internet of Things: The New Frontier for Data Security and Privacy (Part 1)*, INSIDE COUNSEL (Mar. 27, 2015).

75. OWASP Internet of Things Project, OWASP (last viewed Dec. 8, 2015) https://www.owasp.org (follow "More" hyperlink at the top of the page, follow "OWASP Internet of Things Project" hyperlink, click on the "IoT Vulnerabilities" tab at the top of the page).

76. *Id*.

77. HEWLETT PACKARD, *supra* note 12.

78. *Id*.

Further, Hewlett Packard found that 90% of devices collected at least one piece of personal information via the device, cloud, or mobile application that would make exposure risky. Hewlett Packard's study confirmed that with many devices transmitting personal information, much of it unencrypted, by using a home network users are one "misconfiguration away from exposing this data to the world via wireless networks."[79]

Personally identifiable information "PII," is a term used by data professionals and is usually defined as name, address, social security number, or telephone number.[80] Generally, data purveyors need just three data points to know your identity: zip, gender, and date of birth, and they can use this trifecta, the triangulation of data, to reach that identification goal.[81] IoT devices, of course, collect these bits of data and more.[82] The FTC identifies risks related to the IoT as one's sensitive personal information being exposed, which is already something faced by Internet users, but it also notes that there are new risks associated with IoT based on the collection of "habits, locations, and physical conditions over time."[83]

With respect to appropriate data privacy, the FTC's proposed data privacy framework relies on three considerations: (1) a given data set is not reasonably identifiable, (2) the company publicly commits not to re-identify it, and (3) the company requires any downstream users of the data to keep it in de-identified form.[84] If companies meet these considerations, the data would fall outside the scope of the FTC's proposed framework.[85] However, research into the anonymization of IoT data suggests that it is extremely difficult to do so, making uncovering identification far easier than expected.[86] This suggests that IoT data could nominally meet the FTC standards, but practically not conform.[87] Irrespective of the conflicting de-identification research, the FTC contends that the standards applied in HIPAA[88] can result in satisfactory de-identified data sets.[89]

---

79. *Id.*

80. Peppet, *supra* at note 1, at 40.

81. Saad & Field, *supra* note 13.

82. Larry Hardesty, *How Hard Is It to "de-Anonymize' Cellphone Data?* MIT NEWS (Mar. 27, 2013); *see also* Nicholas D. Lane ET AL., *BeWell: A Smartphone Application to Monitor, Model and Promote Wellbeing*, 5TH INTL. ICST CONF. ON PERVASIVE COMPUT. TECH. FOR HEALTHCARE (2015).

83. FTC STAFF REPORT, *supra* note 61.

84. *Id*.

85. Federal Trade Report, *Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers,* FEDERAL TRADE COMISSION 1, 22 (Mar. 2012), https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf.

86. "[D]e-identification has come under increasing pressure by scientists who have demonstrated clever ways to re-identify data, to the point of it being largely discredited by critics." Tene, *supra* note 7.

87. Peppet, *supra* note 1, at 39; Hardesty, *supra* note 82; IoT provides sensor-based data sets in which it is very hard to preserve anonymity.

88. 45 C.F.R. § 164.514(b)(1)

89. FTC STAFF REPORT, *supra* note 61, at 37-8.

Due to the inherent interconnectedness, and the potential risks at all levels, manufacturers and regulators recognize the importance of implementing reasonable security with respect to IoT devices.[90] However, the devices themselves may prevent data privacy and data security by design. Due to the small size of many IoT devices, they may not have sufficient battery life that is required to support robust data security processing, thereby complicating future efforts at consumer protection.[91]

B. Hacks

Devices in IoT systems are connected to a network, which is then exposed to the Internet and thus exposed to Internet hackers.[92] Publicity has already surrounded a number of IoT hacks, for instance, smart automobiles have been hacked to open doors and control engines, helped by videos on the internet explaining how. In the baby monitor "hacking" incident, the only action brought by the FTC related to an IoT device, TRENDnet SecurView cameras sold for home security and baby monitoring, with assurances that they were "secure." However, faulty software in the cameras allowed online viewing by anyone with the cameras' Internet address.[93]

As demonstrated by the publicized hacks, the IoT presents physical and safety concerns with respect to devices used in the home and on a person. The FBI warns that cybercriminals can exploit unsecured wireless connections for IoT devices, including lighting, thermostats, garage doors and security systems, which can allow the criminals to "obtain administrative privileges on the automated device."[94] The FBI points out hackers can expand this limited access to reach a private network, "collect personal information, and even monitor the [IoT] owner's habits and network traffic."[95] The FBI suggests that such access is easier if the IoT owner does not adjust the default passwords for each device.[96]

C. Discrimination

It is clear that the data generated by certain IoT devices and used for analytics will be robust enough to provide a consumer profile that would intrude on areas protected by law from discrimination - employment, healthcare, insurance, and housing. In fact, FTC commissioner Brill has pointed out that "[o]ne of the most troubling risks coming from the collection and use of big

90. Kleine, Lobo & Levendowski, *supra* note 74.
91. Peppet, *supra* note 1, at 43.
92. Berezin, *supra* note 32.
93. *FTC Approves Final Order Settling Charges Against TRENDnet, Inc*., FEDERAL TRADE COMMISSION (Feb. 7, 2014) https://www.ftc.gov/news-events/press-releases/2014/02/ftc-approves-final-order-settling-charges-against-trendnet-inc. Discussed hereafter.
94. Federal Bureau of Investigations, *supra* note 70.
95. *Id*.
96. *Id*.

data is its use in making sensitive predictions about consumers, such as those involving their health conditions, sexual orientation, religion, and race."[97]

The same access to data that allows analytics to produce consumer profiles for marketing, referenced as "risk mitigation" services, may allow for the profiling of consumers in ways that violate existing anti-discrimination laws. For instance, algorithmic scores for "financially challenged" may include data points that also indicate the person's race, whether she is a single-mom, employment status, smoking history, and more. An employer, insurance company, or an intended landlord could potentially use these assessments, built upon data gathered from IoT devices, in a way that interferes with existing law.

D. Ownership

Another disconcerting aspect with respect to the data obtained through the IoT is ownership of that data. The unanswered question is who owns the data? Further, who has rights to access and use it as it flows through the network and cloud? There is not a simple or uniform answer for all devices, and answers will likely require a review of the particular facts surrounding each device. Ultimately, it will probably depend on the specific contract between the parties or there may be trade secret and/or intellectual property overlays.[98] The type of information that comes along with each device or network is likely to take on extraordinary importance when negotiating ownership issues.

The author of Regulating the Internet of Things: First Steps Towards Managing Discrimination, Privacy, Security & Consent purchased or downloaded the user manuals for 20 IoT devices to address the data ownership issue and examine the terms for privacy of data-related information.[99] He found that "none of the twenty devices included privacy or data-related information in the box."[100] He reported that it was also challenging to find privacy data on the websites for the products.[101] Beyond the difficulty finding a privacy policy, he was unable to determine whether these companies shared any personal information or sold it to third parties.[102] More troubling is that while most of the policies he reviewed did not mention ownership of sensor data, the three products in his sample that did discuss ownership "indicated that the manufacturer, not the consumer, owned the sensor data in question."[103]

97. Brill, *supra* note 8, at 210.
98. Berezin, *supra* note 32.
99. *See generally* Peppet, *supra* note 1
100. *Id*. at 56.
101. *Id*. at 57.
102. *Id*. at 58.
103. *Id*., at 60.

VI. AVOIDING POTENTIAL HARM

A.Industry Self-Regulation

At this time, avoiding the potential harms that can result from IoT implementation primarily relies on self-regulation by the industry. Recognizing that security and privacy are essential to earn consumer trust, and that such trust is necessary for customers to adopt the technology, IoT manufacturers and providers have been aggressively pursuing self-regulation with the hope it will earn the approval of the FTC, and will be codified in future legislation. A subset of the industry proposals for a front-line approach is to improve transparency between the user and provider by providing meaningful consents which identify where the data is going. Done with the full support of the FTC, self-regulation is the only protection offered to consumers at this point.

The Electronic Privacy Information Center (EPIC) asserts that "[t]he development of the IoT means that companies preserve privacy. Among other things, this involves adopting privacy and data security best practices, only collecting consumer information with express consumer consent, and providing consumers with access to their data."[104] To this end, the Online Trust Alliance (OTA), an industry think tank, created the IoT Trustworthy Working Group (ITWG) to draft a framework for best practices in security and privacy with respect to the IoT. Established in January 2015, it released the OTA IoT Trust Framework – Discussion Draft, on August 11, 2015 (updated August 13).[105] The ITWG focused on two primary categories: home automation/ home products, and health/fitness wearable technologies.

The fundamental principle underlying the OTA is that its "recommendations are based on Fair Information Practice Principles (FIPPs), notably transparency and data security."[106] FIPPs, which are widely accepted, are the framework of principles "used in the evaluation and consideration of systems, processes, or programs that affect individual privacy. These principles are at the core of the Privacy Act of 1974 and are mirrored in the laws of many U.S. states, as well as in those of many foreign nations and international organizations."[107] The OTA Proposed Minimum Requirements – IoT Trust Framework includes 23 detailed recommendations which it believes should be the "base-

104. EPIC is a public interest research center in established in 1994 to focus emerging privacy issues in the information age. EPIC.ORG (last viewed Nov. 29, 2015), https://epic.org/privacy/internet/iot/.

105. *IoT Trust Framework – Discussion Draft,* OTA (updated Aug. 13), https://otalliance.org/system/files/files/resource/documents/iot_trust_frameworkv1.pdf. The OTA Framework was further updated on November 23, 2015, recognizing again that "'security and privacy by design' must be a priority from the onset of product development and be addressed holistically." The updated framework represents rough consensus following the open comment period.

106. *Id*. at 1.

107. *Id.* at 1, note 1.

line for any self-regulatory and/or certification program."[108] These proposals break down into general categories relating to companies having privacy policies that are accessible, readable, offer full disclosure regarding data collection, and manufacturers must have comprehensive and workable contingency plans for keeping the processes up-to-date and addressing potential attacks.[109] The OTA goes on to make an additional 12 recommendations beyond the framework, most of which mirror the FTC guidance.[110]

However, beyond a generalized agreement that regulation and legislation would stifle invention and growth, there is not complete uniformity among the industry. For instance, with respect to the FIPPs related to notice, choice, access, accuracy, data minimization, security and accountability, arguments have been put forth that they must all apply to the IoT, while others contend that data minimization, notice and choice are impractical in the IoT space.[111] Unfortunately, these differences seemingly leave the industry paralyzed and careless with security to the extent that a large-scale study into the security of such devices conducted in 2015 by the Eurecom research center in France and Ruhr-University Bochum in Germany, revealed significant failures.[112] Eurecom identified significant vulnerabilities in a large number of embedded devices which reveal substandard security testing by manufacturers.[113] Nevertheless, self-regulation, with the support of the FTC, is the best protection offered with respect to the IoT as of mid-2016.

---

108. *Id*. at 2.

109. *Id*. at 2-4.

110. *Id.* at 5. The final version of the report was issued on March 3, 2016. https://otalliance.org/system/files/files/initiative/documents/iot_trust_framework_released_3-2-2016.pdf; The OTA is also publishing a companion resource guide that is in draft form as of April 8, 2016. https://otalliance.org/system/files/files/in-the-news/images/iot_trust_resource_guide_4-8.pdf.

111. Daniel Castro, Statement to the Committee on Energy and Commerce Subcommittee on Commerce, Manufacturing, and Trade, *The Internet of Things: Exploring the Next Technology Frontier,* Hearing (Mar. 24, 2015), http://docs.house.gov/meetings/IF/IF17/20150324/103226/HHRG-114-IF17-Wstate-CastroD-20150324.pdf.

In relevant part: Castro testified that traditional privacy principles do not work in a "big data" world. The FIPPs "such as data minimization – the idea that an entity collecting data should limit the collection of information to what is directly needed to accomplish a specific purpose – are based on the mistaken belief that it is always possible for an organization to predetermine what information is useful and collect only that minimum amount of information. Data-driven innovation often involves exploration and discovery, sometimes from unexpected data sources." *See also* FTC STAFF REPORT, *supra* note 61, at 19 (addressing comments made by industry experts during the FTC's IoT 2013 workshop).

112. Lucian Constantin, *Study Shows Many Embedded Devices Ship Without Adequate Security Tests*, INFOWORLD.COM (Nov. 23, 2015), http://www.infoworld.com/article/3007459/security/study-shows-many-embedded-devices-ship-without-adequate-security-tests.html.

113. Hewlett Packard found similar faults; HEWLETT PACKARD, *supra* note 12.

B. Transparency in Data Collection and Consumer Consent

It is generally believed that best practices with respect to IoT usage will include disclosure and consent policies for each device regarding storage and use, and minimizing the personally information that is collected and the purposes for which it will be used.[114] The FTC echoes the data minimization sentiment which ties in with providing clarity about where the data is disclosed and how it will be used.[115]

However, disclosure, transparency, and consent are severely limited in a practical sense with respect to the IoT. Many of the devices will have no user interface and will function autonomously. For others, when there is no screen, no keyboard, where does one provide such a disclosure? Some suggest clickwrap or another point of purchase download; however, adding more clauses to the current software license agreements (which are usually too long, confusing, and designed to protect the provider) will not be acceptable. Moreover, consumers should be able to direct what types of data they are willing to disclose and be provided with recourse after their PII is exposed.[116] Marc Goodman, author of the book Future Crimes, "characterizes consumers who freely give up their personal data as a result of accepting the conditions contained in the Terms of Service (ToS) agreements with Internet companies, in effect becoming the 'product' not the actual customer."[117] The IoT industry and consumers will need to agree on a balance between their respective interests to resolve this issue.

VII. GOVERNMENT REGULATION

An article co-authored by Samuel Warren and Louis Brandeis in 1890 first enumerated the concept of privacy as a legal interest, describing it as 'the right to be let alone." [118] Such a right is not set forth in the Constitution and Bill of Rights; however, the U.S. Supreme Court has found such a right through its interpretation of the First, Third, Fourth, Fifth and Ninth Amendments. "Privacy achieved hallmark status … with the enactment of the Privacy Act of 1974" which only applied to federal agencies, not the private sector.[119] The general approach to privacy legislation in the U.S. is sectoral. US laws include privacy protections piecemeal into acts addressing specific industries, leaving a laundry list of laws that sprinkle privacy requirements and regulations with-

---

114. Berezin, *supra* note 32.

115. "Ensuring that privacy is woven into the fabric of the Internet of Things requires us to only to think carefully about what data a specific device collects but also about how that data will be used and to whom it will ultimately flow." Brill, *supra* note 8, at 217.

116. Folk, Hurley, Kaplow & Payne, *supra* note 5, at 13.

117. O'Brien, *supra* note 6.

118. Folk, Hurley, Kaplow & Payne, *supra* note 5, at 10 (citing Thomas Cooley, LAW OF TORTS, 2nd ed., Vol. 29, 1888).

119. *Id*.

in the purview of their industry.[120] Theoretically, some of these statutes could protect data generated by the IoT, but, for the most part, IoT specific data, cybersecurity and related privacy issues, will fall through the cracks between the net of individual laws. To date, the FTC has taken the lead with respect to regulating data and the IoT, and other agencies and proposed legislation may advance the process.

A.The Federal Trade Commission

The FTC describes itself as "first and foremost a civil law enforcement agency… the nation's leading consumer protection agency"[121] operating under the authority given in 1938 to protect consumers "from a broad range of unfair or deceptive acts or practices."[122] The FTC has focused on protecting data security and privacy as they give rise to consumer harm by relying on Section 5 of the FTC Act.[123] FTC Commissioner Maureen K. Ohlhausen explained that the Commission files claims for "deceptive acts" which violate Section 5 only if they are material – that is, if they actually harm consumers.[124] And practices are only "unfair" if there is substantial harm that consumers cannot avoid and

120. A list of U.S. Information Privacy Statutes includes:
• California's data breach notification law; Senate Bill 1386 ("SB 1386");
• Children's Internet Protection Act of 2001 (CIPA);
• Children's Online Privacy Protection Act of 1998 (COPPA);
• Communications Assistance for Law Enforcement Act of 1994 (CALEA);
• Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003 (CAN-SPAM);
• Fair and Accurate Credit Transactions Act of 2003 (FACTA);
• Federal Trade Commission Act (FTCA);
• Driver's Privacy Protection Act of 1994 (DPPA);
• Fair Credit Reporting Act of 1999 (FCRA);
• Family Education Rights and Privacy Act of 1974 (FERPA);
• Financial Services Modernization Act of 1999 ("Gramm-Leach-Bliley" or GLBA);
• Privacy Act of 1974;
• Privacy Protection Act of 1980 (PPA);
• Safe Web Act of 2006, bill S.1608;
• Telecommunications Act of 1996;
• Telephone Consumer Protection Act of 1981 (TCPA);
• Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001; H.R. 3162 (USA-PATRIOT);
• Video Privacy Protection Act of 1988.
List compiled by International Association of Privacy Professionals, https://iapp.org/media/pdf/certification/CIPPUS%20Bibliography%202.0-LW-2015-FINAL.pdf.

121. Brill, *supra* note 22, at 1.

122. *Id*.

123. 15 U.S.C. § 45(a).

124. Maureen K. Ohlhausen, FTC Commissioner, "*The Internet of Everything: Data, Networks & Opportunities"* presentation to US Chamber of Commerce Foundation and US Chamber's Center for Advanced Technology & Innovation, Washington, DC (Sept. 22, 2015) 1, 7, https://www.ftc.gov/system/files/documents/public_statements/804001/150922remarkscommmko.pdf.

that outweighs any benefits to consumers or competition."[125]

1.FTC Best Practices for IoT

The FTC hosted an IoT Workshop on November 19, 2013 entitled The Internet of Things: Privacy and Security in a Connected World, which was attended by industry experts and was memorialized in the FTC Staff Report: Internet of Things, Privacy and Security in a Connected World.[126] In sum, the FTC urged workshop participants to address four main FIPPs: security, data minimization, notice, and choice.[127] The FTC laid out a best practices format going forward with respect to data and the IoT.

(1) Security. First, "companies should 'security by design' by building security into their devices at the outset, rather than as an afterthought."[128] Further, companies need to continue to use traditional cybersecurity measures with respect to employees, training, security, etc., and should test security before launching products.[129]

(2) Data Minimization. The FTC, based on suggestions from workshop participants, determined that IoT companies should look closely to determine what data they actually need, and "develop policies and practices that impose reasonable limits on the collection and retention of consumer data."[130] The FTC points out that minimizing data helps guard against at least two types of privacy-related risks to the extent that larger data stores are larger targets for data thieves.[131] Reducing the volume reduces the risk of theft, and, the more data one has, the larger the risk of data used in a manner that is inconsistent with the consumer's reasonable expectations, thus opening the door to unfair practices claims.[132] The FTC also urges companies to keep any data that they must have in a de-identified form if possible, making sure that it cannot be reasonably re-identified.[133]

(3) Notice and Choice. The FTC wants companies to bridge the gap between the physical difficulties associated with providing notice and/or choice on a device without a screen, with the consumer given such a notice and/or choice.[134] Recognizing the practical limitations, the FTC asserts that "provid-

125. *Id.*
126. FTC STAFF REPORT, *supra* note 61.
127. *Id.* at ii.
128. *Id.* at 9
129. "The FTC has emphasized that IoT devices should default to the highest security settings out-of-the-box." *Id.* at 28; "Further, to protect users' sensitive data like financial or medical information from being abused if it is intercepted, the FTC is encouraging companies to encrypt al such information that is shared and stored via their IoT devices." Kleine, Lobo & Levendowski, *supra* note 74.
130. FTC STAFF REPORT, *supra* note 61, at 10.
131. *Id.* at 10.
132. *Id.* at 33-5.
133. *Id.* at 53.
134. *Id.* at 38-39.

ing consumers with the ability to make informed choices remains practicable in the IoT."[135] It suggests video tutorials, QR codes on devices, providing choices at the point of sale, or other approaches which "should be clear and prominent, and not buried within lengthy documents."[136]

(4) Legislation. The FTC specifically states "that IoT-specific legislation at this stage would be premature"[137] and instead asserts that the development of self-regulatory programs "would be helpful as a means to encourage the adoption of privacy- and security-sensitive practices."[138] Instead of IoT-specific legislation, the FTC urges Congress "to enact strong, flexible, and technology-neutral federal legislation to strengthen its existing data security enforcement tools and to provide notification to consumers when there is a security breach."[139] FTC Commissioner Maureen K. Ohlhausen specifically stated: "the FTC's staff report on the Internet of Things appropriately rejected calls for IoT-specific legislation as premature given the lack of any evidence of harms unique to IoT.[140]

Subsequent to issuing its IoT in a Connected World report, in March 2015, the FTC established the Office of Technology Research and Investigation (OTRI) to track "investigative research on technology issues involving all facets of the FTC's consumer protection mission, including privacy, data security, connected cars, smart homes, algorithmic transparency, emerging payment methods, bid data and the Internet of Things."[141] The FTC has set the stage for cooperation with the industry, legislators, and consumers to move forward with implementation of its proposed best practices.

2.FTC Enforcement Actions

The FTC generally handles data privacy and security cases in similar ways.[142] In 2013, the FTC reported that it filed its first action against a marketer of an everyday product with interconnectivity to the Internet and other mobile devices, i.e., Internet of Things.[143] The FTC filed the action against the baby monitor and home security camera company, TRENDnet SecurView, which assured customers that they were "secure," but were actually not. The FTC charged that the company's lax security practices allowed hackers to intrude on its consumers and allowed the public to view their private lives on

135. *Id.* at 39-40.
136. FTC STAFF REPORT, *supra* note 61, at 41-3.
137. *Id*. at 13.
138. *Id*.
139. *Id.* at 49.
140. Ohlhausen, *supra* note 124, at 48-9.
141. Jessica Rich, Bureau of Consumer Protection, Press Release: *BCP's Office of Technology Research and Investigation: The Next Generation in Consumer Protection*, (Mar. 23, 2015), https://www.ftc.gov/news-events/blogs/business-blog/2015/03/bcps-office-technology-research-investigation-next.
142. Scholz, *supra* note 5, at 108, 113.
143. *FTC Approves Final Order Settling Charges Against TRENDnet, Inc*., supra note 93.

the Internet, and ultimately prevailed with a settlement agreement. While the FTC did not file any actions against IoT manufacturers in 2014 or 2015, it is likely there will be more as the technology integrates into society.[144]

The 3rd Circuit ruling in FTC v. Wyndham Worldwide Corp.[145] was arguably the most publicized case involving the FTC's enforcement of data security in 2015.[146] The action alleged that Wyndham, a hospitality company, engaged in unfair and deceptive trade practices under the Act, by failing to maintain appropriate and reasonable data security for consumers' sensitive PII. In response to the District Court's denial of its Motion to Dismiss, Wyndham appealed to the 3rd Circuit, which issued the seminal order upholding the decision of the District Court. The August 2015 ruling has been touted as a victory for the FTC and a ringing endorsement of its authority to regulate data security under the "unfair practices" prong of the FTC Act which prohibits "unfair or deceptive acts or practices in or affecting commerce."[147] However, it is important to note when considering the impact of the decision, the ruling was only in response to Wyndham's motion to dismiss. The case remained in its infancy to proceed through discovery and face the same, or similar, battles in a subsequent motion for summary judgment. At that point, the FTC would have had to prove evidence that Wyndham's cyber-security practices during the relevant period:

1. Caused or were likely to cause substantial injury;

2. That this injury was not reasonably avoidable by consumers themselves; and

3. That this injury was not outweighed by countervailing benefits to consumers or to competition.[148]

The Third Circuit suggested that proof of these elements may not be sufficient, and that the FTC would need to meet its burden of proof regarding unfairness by more than merely identifying instances where Wyndham failed to comply with standards in other FTC settlements. It also stated that the FTC would have to show "substantial injury" to consumers, not just inconvenience.

On meeting the statutory burden of proof, in all cases, the FTC may not be successful with respect to pursuing cybersecurity prosecution. To this end, the FTC suffered a blow on November 13, 2015 when the court dismissed its Sec-

144. Khandekar, *supra* note 6.

145. *FTC v. Wyndham Worldwide Corp.,* 799 F.3d 236 (3rd Cir. 2015).

146. After a three-year battle, Wyndham and the FTC settled this case on December 10, 2015. The terms of the settlement proposed by the parties will be in effect for 20 years, and requires Wyndham to establish a comprehensive information security program for financial data, perform annual security audits, obtain independent certifications of any changes to its data policies and submit to compliance monitoring by the FTC, among other provisions. Notably, Wyndham will not pay a fine to the FTC. *Wyndham Settles FTC Charges It Unfairly Placed Consumers' Payment Card Information at Risk*, FEDERAL TRADE COMMISSION (Dec. 9, 2015), https://www.ftc.gov/news-events/press-releases/2015/12/wyndham-settles-ftc-charges-it-unfairly-placed-consumers-payment.

147. 15 U.S.C. §45(a).

148. 15 U.S.C. §45(n)[2].

tion 5 unfair business practices case against LabMD, brought for failure to implement reasonable and appropriate data security practices. The administrative law judge hearing the case found that it was not enough to demonstrate that harm to consumers was merely possible, but that showings of specific harm were necessary. The FTC alleged that the requirement of the substantial injury to consumers was met by (1) the likelihood of future identity theft of affected consumers, (2) the emotional harm associated with being a data breach victim, and (3) a continued elevated risk of identity theft due to the lax practices of LabMD. The judge rejected all three of these, finding that the specific LabMD facts were too narrow to support such broad assertions.[149] On November 24, 2015, the FTC filed a notice of appeal related to this decision.[150]

The LabMD dismissal, however, was distinguished in the order from the FTC data breach cases against Wyndham and Neiman Marcus.[151] In contrast to LabMD, which immediately reported its finite breach to the FTC, in Wyndham there were three hacks which resulted in $10.6 million of fraudulent charges, and in Neiman Marcus, hackers accessed more than 9,200 customer card numbers and records.[152] While it may give the companies charged optimism, the dismissal of LabMD does not make it certain that the other cases will similarly crumble.

The FTC started 2016 strong with its announcement of its first monetary settlement in a data security case against dental practice supplier, Henry Schein Practice Solutions, Inc.[153] In addition to a 20-year consent order requiring annual compliance reports, Schein will pay $250,000 into a fund to provide those victimized by the encryption failures by the company. The FTC's action focused on Schein's encryption failures and alleged that the company's software was sold "to dental practices around the country with deceptive claims that the software provided industry-standard encryption of sensitive patient information, and, in doing so, ensured that practices using its software would protect patient data."[154] As a result, the dentists using the software

149. Federal Trade Commission Office of Administrative Law Judges, Docket No. 9357, *In the Matter of LabMD INC.,* Respondent, http://causeofaction.org/assets/uploads/2015/11/Docket-9357-LabMD-Initial-Decison-electronic-version-pursuant-to-FTC-Rule-3-51c21.pdf.

150. Complaint Counsel's Notice of Appeal, *In the Matter of LabMD, Inc.*, F.T.C. (No. 9357), 2015 https://www.ftc.gov/system/files/documents/cases/580032_-_labmd_-_complaint_counsels_notice_of_appeal.pdf.

151. *Remijas v. Neiman Marcus Group*, LLC, 2015 U.S. App. LEXIS 12487 (7th Cir. 2015). Motion to dismiss denied on remand, Northern District of Illinois, case no. 1:14-cv-01735.

152. Natasha G. Kohne, Michelle A Reed, David S. Turetsky & Jo-Ellyn Sakowitz Klein, Akin Gump Strauss, Hauer & Feld LLP, *FTC Suffers a Setback in its Quest to Challenge Lax Corporate Cybersecurity Practices: ALJ Dismisses FTC's LabMD Complaint,* Lexology (Nov. 25, 2015), http://www.lexology.com/library/detail.aspx?g=fc839b86-bee1-4d83-a906-2e74afd2eabf.

153. *Dental Practice Software Provider Settles FTC Charges It Misled Customers About Encryption of Patient Data*, FEDERAL TRADE COMMISSION (Jan. 5, 2016), https://www.ftc.gov/news-events/press-releases/2016/01/dental-practice-software-provider-settles-ftc-charges-it-misled.

154. *Id.*

were unable to protect patient data, as required by HIPAA.[155] This case is novel for the monetary recovery, but is consistent with a trend of the FTC pursuing HIPAA violations in its pursuit of protecting privacy under Section 5 of the Act.[156]

B.Federal Communications Commission (FCC)

The Federal Communications Commission ("FCC"), under Section 222 of the Telecommunications Act of 1996 governs privacy of customer information provided to and obtained by telecommunications carriers by imposing restrictions on the access, use, and disclosure of customer proprietary network information (CPNI).[157] Prior to the act, carriers could sell customer data to third-party marketers without consent. The statute imposed new restrictions on the access, use and disclosure of CPNI which restricts providers' ability to disclose CPNI only with consent or as required by law.[158] It is possible that Section 222 will apply to IoT data and be whether IoT data purveyors thus precluded from selling locational and log data to third parties without the knowledge of the IoT users.

The FCC issued an Open Internet Order on February 26, 2015, which went into effect in June of 2015, reclassifying wired and wireless broadband providers from information services carriers subject to Title I of the FCC Act, to broadband service providers subject to Title II of the Act.[159] As Title II carriers, broadband providers like the cable companies Comcast and Verizon, and wireless providers, are subject to regulation just like telephone carriers. IoT data will potentially run on LTE lines, and much of it will certainly process through the Internet, which would subject IoT network providers to Section 222 requirements.

Additional protection against data disclosure is a valid goal. However, the application of the Telecommunications Act to these applications is in its infancy. Verizon appealed the FCC's Open Internet Order to the District Court of Appeals for the District of Columbia Circuit, which sided with the FCC on June 14, 2016. It is assumed that the issue will now be appealed to the U.S. Su-

155. Adam Greene, *As if a 20-Year Consent Order Wasn't Enough Fun: FTC Brings First Monetary Settlement in Information Security Case,* PRIVACY & SECURITY LAW BLOG (Jan. 6, 2016), http://www.privsecblog.com/2016/01/articles/healthcare/as-if-a-20-year-consent-order-wasnt-enough-fun-ftc-brings-first-monetary-settlement-in-information-security-case/.

156. *Id.* "To our knowledge, this is the sixth FTC complaint that has been brought against an entity that is also covered by HIPAA with respect to a health information privacy or security matter."

157. 47 U.S.C. §222 (1996).

158. Peter Swire & Kenesa Ahmad, U.S. PRIVATE-SECTOR PRIVACY, LAW AND PRACTICE FOR INFORMATION PRIVACY PROFESSIONALS, 100 (2012).

159. FCC Open Internet Order (Feb. 26, 2015) https://www.fcc.gov/openinternet.

preme Court for a final determination.[160] While net-neutrality is the key issue in the Open Internet Order,[161] it will bleed over into regulating the IoT to the extent that §222 of the FCC Act protects consumer privacy and "demands that every telecommunications carrier take reasonable precautions to protect the confidentiality of its customer's proprietary information."[162] Information service providers under Title I have no such requirements, making the outcome of the final appeal relevant to adding another level of privacy protection for the IoT.[163]

Like the FTC, the FCC has started to bring data security cases. The FCC settled its first data security and privacy enforcement action against a Title II cable operator – Cox Communications – in November 2015.[164] The FCC brought the action against Cox for failing to protect customers' PII in 2014 when it was subject to a data breach by a hacker demonstrates its willingness to use enforcement actions pursuant to the Act to protect data privacy.[165]

After this settlement, on November 16, 2015, the FTC and the FCC entered into the "FCC-FTC Consumer Protection Memorandum of Understanding" wherein the two agencies agreed to coordinate and consult with each other regarding complaints, investigations and the overlapping marketplace practices when regulating the "deceptive, unfair, unjust and/or unreasonable" acts and practices of common carriers. [166] The agencies agreed to both share data and to "engage in joint enforcement actions, when appropriate."[167]

On March 31, 2016, the FCC, without waiting for a final ruling on the 2015 Open Internet Order, went a step further by adopting a Notice of Proposed Rulemaking ("NPRM") to establish privacy rules for Broadband Internet Access Service providers.[168] It proposes they add a new subpart to the Code of Federal Regulations (Section GG, 47 C.F.R. §64.7000 et seq.) which would ad-

---

160. Joseph Avanzato, *D.C. Circuit Upholds FCC's Net Neutrality Rules*, JD SUPRA BUSINESS ADVISOR (June 28, 2016) http://www.jdsupra.com/legalnews/d-c-circuit-upholds-fcc-s-net-45910/

161. *Id.* The goal of the Open Internet Order was adopted to "prevent blocking, throttling, paid prioritization and anything designed to harm internet openness."

162. 47 U.S.C §222(a).

163. Marguerite Reardon & Roger Cheng*, FCC Strikes in Net neutrality war: Run Internet like a Utility*, C/NET BLOG, (Feb. 4, 2015), http://www.cnet.com/news/fcc-chairman-wheeler-to-use-utility-style-rules-to-enforce-net-neutrality/.

Cox Communications to Pay $595,000 to Settle Data Breach Investigation, FEDERAL TRADE COMMISSION (Nov. 5, 2105), https://www.fcc.gov/document/cox-communications-pay-595000-settle-data-breach-investigation-0.

165. *Id.*

166. *FCC, FTC Sign MOU on Consumer Protection Cooperation*, FEDERAL TRADE COMMISSION (Nov. 16, 2105) https://www.fcc.gov/document/fcc-ftc-sign-mou-consumer-protection-cooperation-0.

167. *FCC-FTC Consumer Protection Memorandum of Understanding*, FEDERAL COMMUNICATIONS COMMISSION, FEDERAL TRADE COMMISSION, (Nov. 16, 2015) https://apps.fcc.gov/edocs_public/attachmatch/DOC-336405A1.pdf.

168. FCC 16-39 In the Matter of: Protecting the Privacy of Customers of Broadband and Other Telecommunications Services, NPRM available at: https://apps.fcc.gov/edocs_public/attachmatch/FCC-16-39A1.pdf.

dress proprietary data as well as PII. The NPRM, based on principles that are consistent with the FTC's mandate, focuses on transparency, choice, and security. The NPRM contains proposals for data breach notification standards and suggests a harmonization with traditional telecom, VoIP, cable, and satellite rules. The proposed rules, which are out for comments through the end of June 2016, will impact the IoT since, as discussed previously in this paper, much of the IoT data will transfer through internet and broadband providers.

C. Fair Credit Reporting Act of 1999 (FCRA)

The Fair Credit Reporting Act ("FCRA")[169] establishes consumer rights regarding credit reports. Consumer reporting agencies (CRAs), which assemble and evaluate consumer data to prepare reports for 3rd parties, provide reports bearing on a consumer's "credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living which is used" to establish a consumer's eligibility for credit, insurance or employment purposes.[170]

The question is whether data mined from IoT devices, then analyzed and sold, makes an IoT data seller a CRA under the FCRA. If so, then consumers will have a number of rights under the act to gain access to their reports and dispute the accuracy of the info provided. As CRA's, IoT providers would also have additional duties under the Act to take reasonable steps to ensure accuracy, limit reporting of negative information, provide consumer assistance, provide customers with notice, and provide consumer reports only to entities that have a permissible purpose under the FCRA.[171] If they are not CRAs, but are just "furnishers" of info to CRAs, then the FCRA forbids them from knowingly reporting inaccurate information.[172] The classification of the IoT data provider is important because it must either produce accurate information to a CRA, or, as a CRA, publish the information and then give the consumer the right to dispute.

FCRA reports may only be disclosed to certain "users" which include employers, lenders, insurers and others who rely on the reports to make employment, housing, lending and insurance decisions. Thus, whether IoT providers transmit data into a credit report as a CRA directly, or as a "furnisher" of data to a CRA, that data could impact areas that are protected from discrimination. Another level of potential risk relates to investigative consumer reports which contain information about a consumer's character, general reputation, personal characteristics, and mode of living.[173] IoT data will be ripe with much of this information, without the need for personal interviews that

169. 15 U.S.C. 1681, *et. Seq* (1970).
170. Peppet, *supra* note 1, at 36-7.
171. 15 U.S.C. §1681i(a)(1)(A).
172. 15 U.S.C. §1681s-2(1) (A-B).
173. 15 U.S.C. §1681d.

are now required to create an investigative consumer report. If a user intends to obtain such a report, it must be disclosed to the consumer, in writing, providing the consumer with notice of his/her rights.

The implications of FCRA application are separate from those related to any FTC protections. While the FTC's goals are to protect privacy of data, the purpose of the FCRA is to address the correctness and dissemination of appropriately shared data. The FCRA is also designed to ensure accuracy in credit reports. However, accuracy may not be the actual issue with respect to IoT sensor data because IoT data is inherently accurate. Thus, there will be little to challenge for accuracy. Rather, the inferences drawn from such data are likely to cause the problems and disputes[174] and FCRA is not presently equipped to accommodate any such inferences. "Thus, FCRA provides consumers with little remedy if IoT data were to be incorporated into the credit reporting processes."[175]

The FTC, state attorneys general and, pursuant to the Dodd-Frank Wall Street Reform and Consumer Protection Act, the Consumer Financial Protection Bureau ("CFPB") enforce FCRA violations, and individuals have private rights of action and statutory damages remedies. To the extent that the FCRA regulations can extend to cover IoT data, questions about how such actions were expected to be addressed by the Supreme Court in the data-privacy case Spokeo, Inc. v. Robins.[176] Spokeo is a putative class case under the FCRA 15 U.S.C. § 1681 based on inaccurate personal information being placed in a credit report. Spokeo presents a novel issue, which is also its biggest hurdle – the misinformation related to the lead plaintiff was actually favorable to the extent that the offending report described him as wealthier and better-educated that he actually is in reality. Irrespective of such flattery, he brought the claim for the statutory damages against a reporting agency that failed to "follow reasonable procedures to assure maximum possible accuracy" [177] of consumer data. The plaintiff claims that he suffered an "injury in fact" based on the knowledge that false information about him caused him emotional distress, sufficient to meet the Article III Constitutional standing requirement. Court watchers anticipated that the Justices would decide whether false data in a report must be false, actually published, and/or have caused verifiable injury.

Instead, the ruling, which was the cause for much speculation in the wake of Justice Antonin Scalia's death, was a punt on the standing issue. On May 16, 2016, the Supreme Court, issued a 6-2 opinion remanding the case.[178] The court held that the Ninth circuit, which only focused on the "particularization" prong in its Article III standing analysis, must reevaluate the case to deter-

174. "[T]he main privacy issue is not identity but rather inference." Tene, , *supra* note 5.
175. Peppet, *supra* note 1, at 37.
176. *Spokeo Inc. v. Robins*, U.S., No. 13-1339; *Robins v. Spokeo, Inc.*, 742 F.3d 409 (9th Cir. 2014).
177. 15 U.S.C. §1681e(b).
178. *Robins*, 136 S. Ct. at 1540.

mine whether the injury in fact was also "concrete." While a ruling was expected to give guidance and possibly impact the protection that IoT providers need to extend to their consumers, and thereby heighten or lessen their burden for ensuring accurate reporting of the data collected by consumer use of IoT, the remand order leaves the issue open for another day.

D. The Consumer Financial Protection Bureau ("CFPB")

Relying on the authority granted to the agency by the Dodd-Frank Act to take action against institutions engaged in deceptive practices, the CBPB has entered into its first data security/data privacy enforcement. The Bureau announced on March 2, 2016 that it had issued a $100,000.00 civil fine against Dwolla, Inc., an online payment platform, for deceiving customers about the company's data security systems for protecting sensitive personal information.[179] Dwolla collects personal information, including name, address, date of birth, social security number and bank account information, much of which IoT providers also collect. This suggests that financial data collected and processed through IoT devices may also face limited review, and potential prosecution, by the CFPB if its data security practices are not as promised.

E. Other Governmental Agency Guidance on IoT Technology

1. The Department of Commerce - NIST Framework

The Department of Commerce's National Institute of Standards and Technology ("NIST") released a draft Framework to Help Cyber Physical Systems Developers on September 18, 2015,[180] which it opened for public comment. The NIST framework refers to IoT devices as Cyber Physical Systems ("CPS") and attempts to set forth a common foundation for technology across industries, including transportation, energy, healthcare and manufacturing. It addresses privacy and security challenges presented by an interconnected world and recognizes that the data generated by the IoT may not be the same as in a typical data breach.[181] NIST warns beyond privacy violations to potential physical damage, and, like the FTC, urges industry self-regulation to reduce the risks inherent in the products by considering "what gains may be had in collecting and maintaining certain data versus the risks and compliance

179. *CFPB Takes Action Against Dwolla for Misrepresenting Data Security Practices,* CONSUMER FINANCIAL PROTECTION BUREAU (Mar. 2, 2016), http://www.consumerfinance.gov/newsroom/cfpb-takes-action-against-dwolla-for-misrepresenting-data-security-practices/.

180. *NIST Releases Draft Framework to Help 'Cyber Physical Systems' Developers,* NIST (Sept. 18, 2015), http://www.nist.gov/el/nist-releases-draft-framework-cyber-physical-systems-developers.cfm. For updated status of the NIST working group see also: https://pages.nist.gov/cpspwg/.

181. *Id.*

costs associated with data collection."[182]

2. Federal Food and Drug Administration

The Food and Drug Administration ("FDA") released a draft guideline for IoT devices on January 15, 2016, for design considerations and recommendations for interoperable medical devices, which addresses data collection and data security concerns and recommendations.[183] The FDA uses the 2014 NIST guidelines as its basis for cybersecurity recommendations to IoT medical device manufacturers.[184] Similarly to the FTC and NIST, the FDA relies on self-regulation for those creating and supplying the IoT technology to build products that protect data and data security.[185]

F.Congressional Proposals

1.IoT Legislation

In 2015, the Internet of Things was the subject of specific hearings and a Senate resolution. On February 11, 2015, the U.S. Senate Committee on Commerce, Science, and Transportation held a full committee hearing, "The Connected World: Examining the Internet of Things."[186] A month later, on March 24, 2015, the Senate unanimously approved a bipartisan "The Internet of Things" Resolution to promote greater consumer empowerment and economic growth in the connected world.[187]

That same day, on March 24, 2015, the U.S. House of Representatives En-

182. Carlton Fields, *NIST IoT Framework Raises Interesting Cybersecurity and Data Privacy Challenges*, LEXOLOGY (Dec. 23, 2015), http://www.lexology.com/library/detail.aspx?g=6ddd0cc7-231c-42dc-ad1c-0c226aae5091.

183. *FDA outlines cybersecurity recommendations for medical device manufacturers*, U.S. FOOD AND DRUG ADMINISTRATION (Jan. 15, 2016) http://www.fda.gov/NewsEvents/Newsroom/PressAnnouncements/ucm481968.htm; Report available at http://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/UCM482022.pdf.

184. *Id.*

185. Zachary Brennen, *Interoperable Medical Devices: FDA Offers Design, Labeling Considerations*, RAPS REGULATORY AFFAIRS PROFESSIONALS SOCIETY (Jan. 25, 2016), http://www.raps.org/Regulatory-Focus/News/2016/01/25/23964/Interoperable-Medical-Devices-FDA-Offers-Design-Labeling-Considerations/; Yarmela Pavlovic, Jennifer Agraz Henderson & Lina Kontos, *FDA Offers New Recommendations for Interoperability of Connected Devices,* LEXOLOGY (Feb. 1, 2016), http://www.lexology.com/library/detail.aspx?g=52b788b8-fdf1-4434-bfc6-722812f086d8.

186. *The Connected World: Examining the Internet of Thing,* U.S. SENATE, COMMITTEE ON COMMERCE, SCIENCE, AND TRANSPORTATION, (Feb. 11, 2015) http://www.commerce.senate.gov/public/index.cfm/2015/2/the-connected-world-examining-the-internet-of-things.

187. *Senate Passes Booker's Bipartisan "Internet of Things" Resolution* COREY BOOKER, UNITED STATES SENATOR FOR NEW JERSEY (Mar. 25, 2015), http://www.booker.senate.gov/?p=press_release&id=222.

ergy & Commerce Committee, Subcommittee on Commerce, Manufacturing, and Trade held its own hearing on the Internet of Things and heard testimony from industry representatives and corporate leaders regarding Internet-connected devices and the benefits thereof. At the hearing, both Congress and the private sector recognized the need for privacy protection. Nevertheless, Daniel Castro, Vice President of the Information Technology and Innovation Foundation, an industry trade organization, cautioned against passing privacy laws prematurely that might stifle innovation.[188] Rose Schooler, Vice President of the IoT Group at Intel Corporation echoed Castro's concerns, while also supporting the FTC position that security should be considered at the outset at all levels where breaches might occur.[189]

Subsequently, on June 23, 2015, a group of U.S. senators sent a letter to the Government Accountability Office (GAO) calling for it to explore the Internet of Things, including the opportunities and challenges surrounding the technology, and asking the GAO to study to the technical standards necessary for devices to communicate with users and each other.[190] Most recently, on July 29, 2015, the U.S. House of Representatives, Subcommittee on Courts, Intellectual Property, and the Internet held a hearing on the current and future challenges facing the Internet of Things.[191]

Continuing with attempts to protect IoT consumers, specifically consumers of connected vehicles, Senators Edward Markey and Richard Blumenthal,[192] and Representatives Joe Wilson and Ted Lieu,[193] proposed legislation

---

188. Castro, *supra* note 111; "Policymakers should be extremely cautious about passing laws on the basis of purely speculative concerns that might not even come to pass, especially when doing so might curtail substantial economic and societal benefits, many of which are already being realized today."

189. Michael C. Burgess, *The Internet of Things: Exploring the Next Technology Frontier*, U.S. HOUSE, SUBCOMMITTEE ON COMMERCE, MANUFACTURING, AND TRADE (March 24, 2015) http://docs.house.gov/meetings/IF/IF17/20150324/103226/HHRG-114-IF17-20150324-SD004.pdf; *#SubCMT Taps into the Next Technology Frontier: The Internet of Things,* ENERGY AND COMMERCE COMMITTEE (Mar. 24, 2015) http://energycommerce.house.gov/press-release/subcmt-taps-next-technology-frontier-internet-things#sthash.hpaZm49l.dpuf; Ani Gevorkian, *House Holds Internet of Things Hearing*, THE NAT'L L. REV. (Mar. 30, 2015) (Her position, and that of the FTC, is that security protections should be built into the device, the network and the cloud).

190. *Bipartisan Group of Senators Sends Letter to GAO, Calling for Study of the "Internet of Things",* DEB FISCHER, UNITED STATES SENATOR FOR NEBRASKA (June 23, 2015) http://www.fischer.senate.gov/public/index.cfm/2015/6/bipartisan-group-of-senators-sends-letter-to-gao-calling-for-study-of-the-internet-of-things.

191. O'Brien, *supra* note 6.

192. S. 1806 – SPY Car Act, July 21, 2015 (requires the National Highway Traffic Safety Administration (NHTSA) to cooperate with the FTC to establish standards for data privacy and computer network security to prevent hacking of vehicles manufactured in the U.S).

193. Examining Ways to Improve Vehicle and Roadway Safety: Vehicle Data Privacy. Proposes to develop privacy policy regarding data generated by connected car usage, and would require filings with the Secretary of Transportation and a new Automotive Cybersecurity Advisory Council to be created by the NHTSA. *Committee Releases Draft Proposal to Keep Families Safe on the Road*, THE ENERGY AND COMMERCE COMMITTEE (Oct. 14, 2015). http://energycommerce.house.gov/press-release/committee-releases-draft-proposal-keep-families-safe-road.

in the second half of 2015 to protect IoT data privacy generated by the use of smart cars. Each proposal seeks to involve the National Highway Traffic Safety Administration ("NHTSA") into the privacy oversight process, and yet again the FTC cautioned against IoT specific legislation in favor of self-regulation.[194]

2.Privacy Legislation

The FTC urged Congress to pass general technology-neutral data security legislation to protect against unauthorized access to (1) PII and (2) devices themselves. The FTC

> [R]ecommends that Congress consider enacting broad-based (as opposed to IoT-specific) privacy legislation. It asserts that such legislation should be flexible and technology-neutral, while also providing clear rules of the road for companies about such issues as when to provide privacy notices to consumers and offer them choices about data collection and use practices.[195]

Since then, there has been bipartisan movement in the Senate and House to advance general data privacy legislation. On April 15, 2015, Democratic Senator Thomas Carper of Delaware introduced S.961 – Data Security Act of 2015, in the 114th Congress, which would require non-government entities that handle nonpublic PII to create and implement security programs and to notify law enforcement, consumer reporting agencies, and consumers of data breaches of unencrypted information that may cause identity theft. On May 1, 2015, Republican Representative Randy Neugebauer of Texas introduced similar legislation to the House [H.R.2205 – Data Security Act of 2015] thereby showing bipartisan and bicameral support for improved data privacy protection laws.

F.Executive Action

The Executive Office of the President has also weighed in on the issues of big data[196] and consumer privacy. On February 27, 2015, President Obama's administration circulated a discussion draft of a "Consumer Privacy Bill of Rights Act of 2015" addressing personal data, transparency/consents, individual control of data, collection and responsible use, security, accountability and enforcement.[197] The stated purpose of the proposed legislation is "to es-

194. FTC STAFF REPORT, *supra* note 57; Ohlhausen, *supra* note 104; *see also* Automobiles: F. Paul Pittman, *Legal Developments in Connected Car Arena Provide Glimpse of Privacy and Data Security Regulation in Internet of Things,* DATAPRIVACYMONITOR.COM (Feb. 2, 2016) http://www.dataprivacymonitor.com/online-privacy/legal-developments-in-connected-car-arena-provide-glimpse-of-privacy-and-data-security-regulation-in-internet-of-things/.

195. FTC STAFF REPORT, *supra* note 61, at 50.

196. EXECUTIVE OFFICE, *supra* note 58.

197. *See* EXECUTIVE OFFICE OF THE PRESIDENT, *Administration Discussion Draft: Consumer Privacy Bill of Rights Act of 2015* (Feb. 27, 2015)

tablish baseline protections for individual privacy in the commercial arena and to foster timely, flexible implementations of these protections through enforceable codes of conduct developed by diverse stakeholders."[198] It has faced criticism from the industry for going too far,[199] and from the FTC for not going far enough, and Congress did not pass it in the 2015 legislative year.[200]

G.Other Legislation

1.Health Insurance Portability and Accountability Act of 1996

The Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), Public Law 104-191, addresses data privacy regarding medical records, applying to "covered entities" which include healthcare providers, health plans/insurers, and healthcare clearinghouses, and creates obligations for their "business associates." Health information in the hands of anyone else is not protected by HIPAA. The FTC recognized this limitation in its IoT report, stating that "consumers should have transparency and choices over their sensitive health information, regardless of who collects it. Consistent standards would also level the playing field for businesses."[201] Further, the AFCEA has question the ownership of health data related to IoT devices and whether HIPAA will apply to data obtained from devices like the Fitbit or insulin pumps.[202] In the meantime, the FTC continues to pursue actions for data protection violations related to the HIPAA Security Rule[203] for specific violations of the Department of Commerce's National Institute of Standards and Technology ("NIST")[204] standards.[205]

2.Children's Online Privacy Protection Act of 1998

The Children's Online Privacy Protection Act of 1998, COPPA, imposes certain requirements on website operators or online services that are di-

---

https://www.whitehouse.gov/sites/default/files/omb/legislative/letters/cpbr-act-of-2015-discussion-draft.pdf.

198. *Id*. at 1.

199. *Tech Industry Response to the President's Discussion Draft Privacy Proposal* THE INFORMATION TECHNOLOGY INDUSTRY COUNCIL (Feb. 27, 2015) http://www.itic.org/news-events/news-releases/tech-industry-response-to-the-president-s-discussion-draft-privacy-proposal.

200. Lan Du & Katherine Kwong, *White House Releases Administration Discussion Draft for Consumer Privacy Bill of Rights Act of 2015*, JOLT DIG., HARV. J. OF L. & TECH. (Feb. 27, 2015).

201. FTC STAFF REPORT, *supra* note 61, at 52.

202. Folk, Hurley, Kaplow & Payne, *supra* note 5.

203. "The HIPAA Security Rule establishes national standards to protect individuals' electronic personal health information that is created, received, used, or maintained by a covered entity. [It] requires appropriate administrative, physical and technical safeguards to ensure the confidentiality, integrity, and security of electronic protected health information." 45 CFR 160, 164. : http://www.hhs.gov/hipaa/for-professionals/security/index.html.

204. http://www.nist.gov/index.html.

205. Greene, *supra* note 155.

rected to children under 13, and on operators' websites and online services that have actual knowledge that they are collecting personal information online from a child under.[206]

The FTC began warning foreign app developers that they must comply with COPPA's rules related to obtaining verifiable parental consent for obtaining information from minors.[207] In particular, in December 2014 the FTC sent BabyBus, a China-based mobile app developer of educational apps marketed to young children, a warning because some of the apps collect geolocation information shared with analytics companies.[208] Despite warnings, the FTC has not brought enforcement actions against foreign developers, but has taken the position that COPPA has international reach, and such actions may come in the future.[209]

The leaders of the US Congressional Privacy Caucus and a number of Attorneys General have gone a step further, opening investigations and issuing a letter to VTech, a maker of kids' technology, after VTech disclosed an IoT breach in December 2015. VTech's "Kid Connect" was hacked and the malefactors gained access to PII of more than 4.8 million parents and 6.4 million children, including kid selfies and voice recordings.[210] It is possible that COPPA, which has more stringent privacy requirements for children than the general public, may be used with greater ferocity with respect to IoT data.

3.State Laws

There is a patchwork of state laws that apply to data security which are not uniform, sometimes inconsistent with each other, and enforced individually by each state's attorney general. Almost all of the state laws exclusively apply retroactively to past breaches and do not address proactive steps for avoiding data breaches. Further, it is not clear whether the IoT even qualifies in the state law enforcement regime. Most state statutes apply just to PII (an individual's first and last name plus one or more of: driver's license number, bank or credit card account information, or their social security number). However, a breach of data that resulted in a theft of names plus personal data that is not traditional PII, for instance biometric or sensor data from health monitors or home appliances, may not trigger state data breach notification requirements, even though thousands of users could be put at physical risk for

206. 16 CFR Part 312.

207. Lindsey Tonsager, *FTC Warns Foreign Mobile-App Developer to Comply with COPPA,* THE NAT'L L. REV., (Jan. 9, 2015).

208. Id.

209. Id.

210. Jim Finkle, *After Hack, Congress Wants to Know How VTech Collects Data on Kids*, THE HUFFINGTON POST (Dec. 3, 2015), http://www.huffingtonpost.com/entry/hack-vtech-collects-data-on-kids_us_565f3651e4b08e945fedae8a.

Manatt Phelps & Phillips LLP, *Data Breach Triggers Concerns About IoT Technology and COPPA,* LEXOLOGY (Dec. 18, 2015), http://www.lexology.com/library/detail.aspx?g=f675f06e-03b2-42d3-a2bc-23005d3c5e63.

their safety or home protection.[211]

California leads the way with respect to data privacy legislation. California – A.B. 1116 passed in October 2015, makes it the first to regulate the internet of things by requiring manufacturers of smart-TV's to ensure that the TV's do not record peoples' voices for advertisement purposes. It requires that consumers consent before the voice-recognition features can be enabled, and mandates that obvious warnings be given to people using the Internet connected TV's informing them that their voices could be recorded and sent to the manufacturer or even to third-parties.[212]

Illinois seemingly has the most protective statute regarding the protection of biometric data, the Biometric Information Privacy Act ("BIPA").[213] Illinois enacted the statute protect residents of Chicago, which was serving as a test city for the use of biometric data like fingerprint identification, and has a broad definition of biometric data that may transcend into IoT applications.[214] BIPA, which requires written data retention policies and consent from consumers before colleting biometric information, was the basis for at least four class action cases for the collection of facial recognition and fingerprint data. In December of 2015, one of these cases which was filed against Shutterfly for use of photo facial recognition features without consumer consent, sustained a motion to dismiss and will proceed with discovery,[215] leaving the plaintiffs' likely to continue filing no-harm class actions with potentially crippling statutory damages.

VIIII. PRIVATE LITIGATION

Attorneys and analysts suggest that private litigation may ultimately shape the way that the IoT is regulated to the extent that the potential for civil

---

211. Peppet's review of the 46 state laws enacted in 2014 revealed that just three states and Puerto Rico included a limited definition of medical information in their data breach statutes, and just four mention "unique biometric data" in their definitions of "personal information." Peppet, *supra* note 1, at 46-47.

212. Chad M. Mandell & LeClair Ryan, *When It Comes to Privacy Laws, California leads the Way,* JDSUPRABUSINESSADVISOR.COM (Nov. 23, 2015) http://www.jdsupra.com/legalnews/when-it-comes-to-privacy-laws-61386/.

213. 740 ILCS 14/ (2008)

214. 740 ILCS 14/10 (2008)

"Biometric identifier" means a retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry. . .

"Biometric information" means any information, regardless of how it is captured, converted, stored, or shared, based on an individual's biometric identifier used to identify an individual. . .

"Confidential and sensitive information" means personal information that can be used to uniquely identify an individual or an individual's account or property. Examples of confidential and sensitive information include, but are not limited to . . . a unique identifier number to locate an account or property, an account number, a PIN number, a pass code, a driver's license number, or a social security number.

215. *Norberg v. Shutterfly, Inc*., Case No. 15-cv-5351 (N.D. Ill.).

liability will serve as a deterrent to lax security and privacy.[216] To this end, manufacturers whose policies, or lack thereof, allow data breaches to occur will not only face the potential wrath of the FTC, but also from the plaintiffs' class action bar. Data breach civil class cases have been brought against big retailers The Home Depot, Neiman Marcus and Target as a result of the large security breaches they allowed, as well as dozens of other companies whose data was breached.

The Home Depot[217] and Target[218] are both defending security breach litigations brought by two classes of plaintiffs – consumers and financial institutions. Target previously settled an uncertified class action case brought by consumers, but, faced hirer litigation risks after the federal judge in Minnesota hearing the case certified a class of financial institutions who claim out of pocket expenses related to covering for the actual fraud caused by the data theft. The Court held that the plaintiff banks had to issue "nearly every card" subject to a post-breach alert, and that the banks bore the cost of the issue due to Target's breach, therefore, the plaintiffs did not merely suffer a "risk of future harm" as alleged by Target.[219] Following the order, on December 2, 2015, the parties filed a revised preliminary settlement request for approval.[220]

Despite these moderate advancements for class cases where individuals have suffered quantifiable harms, many privacy-related class action cases are facing an uphill battle with respect to standing. The obstacle is whether class cases will be able to move forward without actual harm to the consumers.[221] Companies are relying on the standard set by the Supreme Court in Clapper v.

---

216. Andrew Phillips & Alexander Madrid, *Vizio and Google Data Privacy Class Actions Illustrate Risks of Data Collection – And Defensive Value of Robust Disclosures*, JDSUPRA BUSINESS ADVISOR (Dec. 1, 2015), http://www.jdsupra.com/legalnews/vizio-and-google-data-privacy-class-13090/; Kimberly Dempsey Booher, Susan M. Freedman, R. Mark Halligan, Martin B. Robins & Alan S. Wernick, *Privacy and Security: PCI's, Class Actions, Cookies and Safe Harbors*, LEXOLOGY (Dec. 18, 2015) http://www.lexology.com/library/detail.aspx?g=a9125398-cd88-4191-95f7-2e119e3c9815; Kristin Ann Shepard, *Data Breach Class Actions: 2015 Year in Review and 2016 Preview,* CLASSIFIED: THE CLASS ACTION BLOG (Dec. 15, 2015), http://classifiedclassaction.com/data-breach-class-actions-2015-review-2016-preview/; John Hutchins, Privacy vs. Data Security: Why Plaintiffs in Consumer Data Breach Cases Still Have a Long Way to Go, JDSUPRA BUSINESS ADVISOR (Jan. 27, 2016), http://www.jdsupra.com/legalnews/privacy-vs-data-security-why-plaintiffs-86759.

217. David Allison, *Home Depot Given Until July to Respond to Data Breach Lawsuits*. ATLANTA BUSINESS CHRONICLE (Jan. 20, 2105).

218. *In re: Target Corp. Customer Data Security Breach Litigation*, MDL Case No. 14-2522, 2015 U.S. Dist. LEXIS 123779 (D.Minn. 2015).

219. *Id*. at *10-11.

220. *Id.*

221. See *Spokeo* discussion above, wherein the Supreme Court is deciding how much harm is necessary to have standing to bring a class case, as well as BIPA cases where it remains to be seen if biometric data class cases can move forward without harm; David Almeida & Mark Eisen, *Tag, You're It: Biometric Information Privacy Act Class Action Against Shutterfly Moves Past 12(b)(6)* NATIONAL LAW REVIEW (Feb. 1, 2016) http://www.natlawreview.com/article/tag-you-re-it-biometric-information-privacy-act-class-action-against-shutterfly?sthash.mddGZ6FT.mjjo.

Amnesty Int'l,[222] that a plaintiff must allege a "concrete and particularized" and "actual or imminent" harm to establish standing. The ruling of the U.S. Supreme Court in Spokeo in 2016 was expected to strengthen or weaken this defense, however, the issue was remanded with instructions to analyze both concrete and particularized to determine Article III standing. If the class plaintiffs and their counsel are successful on remand, and the cases survive motions to dismiss and motions for class certification, it is likely that there will be multi-million dollar settlements by the data offenders. In the event that this occurs, companies will be forced to recognize the risks, costs and liability associated with being cavalier with consumer data. However, before that occurs, it is likely that the issue will be presented to the Supreme Court again.

The class action bar has taken on the role of private Attorneys General, or a private FTC, to pursue those who harm consumers by mishandling their PII. As these cases erupt swiftly in response to address specific harm to consumers, the class bar will be able to address IoT breaches, defects and other shortcomings in real time instead of trudging through the legislative process. In the system of checks and balances, the economic result of civil liability will lead companies to spend money developing safer products with high safeguards for protecting consumer data, rather than paying out legal claims. In effect, civil litigation will support and advance self-regulation by the industry.

VIX. CONCLUSION

The IoT is the next frontier in technological advancement and will change the way we live over the course of the next generation and beyond. As society quickly moves from the adoption today of Fitbits and smart TVs, to the integration of autonomous cars and smart grids running our home energy and utility consumption, and continues on to incorporate other advancements that we cannot yet imagine into our lives, laws to protect us are slowly evolving. Legal scholarship to this point has focused mainly on finite issues, whether it is product specific,[223] or general privacy issues. The bulk of writing on the IoT is from law firm client newsletters, blogs, industry reports, and trade publications.

This paper compiled information from the various sources, legal scholarship, government agencies and legislation, and industry publications, to provide an overview of the technology as it stands in the middle of 2016 and assessed the potential regulations and laws that may apply to consumers. However, continued monitoring and evaluation is required as the devices ad-

222. *Clapper v. Amnesty International*, 133 S.Ct. 1138 (2013). Case brought by plaintiffs seeking proactive relief from the spying on foreign citizens permitted under the Foreign Intelligence Surveillance Act of 2008 ("FISA") (50 U.S.C. Sec. 1881). The Court held that plaintiffs failed to demonstrate the future injury they purportedly feared was certainly impending, that it was traceable to FISA or that the costs incurred to avoid any surveillance were traceable to FISA.

223. Zachary Brennen, *supra* note 183 (medical devices); Collis, *supra* note 30 (energy); Tonsager, *supra* note 205 (mobile apps).

vance and integrate into everyday use, and, as the struggle between the different agencies and different branches of government seek to exert power over regulation and legislation. General data privacy laws related to PII, the most likely area for swift legal development, will need to assessment as they relate to the new data that will be generated by the IoT, and suggestions for how to protect the new classes of data will be required.

Fortunately, there is recognition by the IoT industry, Congress, the President and the applicable administrative agencies, like the FTC, that regulatory guidance and consumer privacy protections are necessary. Even though the concepts of technical growth and the need for applicable laws that both protect people and encourage development are moving in the same direction, the IoT is accelerating a warp speed, while regulation is merely progressing at an organic pace. Stronger cybersecurity and privacy laws, especially those with broad data and PII definitions that can morph to accommodate the varied types of data that will be produced by the IoT (rather than letting it through the current cracks in our privacy system) will be the best first step towards protecting consumers as the world adopts the IoT.