VOLUME 24 FALL 2018

ILLINOIS BUSINESS LAW JOURNAL

TOUCHING THE UNTOUCHABLES: REGULATING THE INTERNET OF THINGS INDUSTRY IN LIGHT OF THE EUROPEAN UNION'S UPCOMING E-PRIVACY REGULATION

❖ NOTE ❖

Clinton Oppong *

I. INTRODUCTION

Sometimes things seem all too familiar when what we see on television becomes perceptible in our lives. *Spoiler alert!* Facebook's sharing of its user data with Cambridge Analytica[1] reminds many of the plot of Westworld,[2] HBO's acclaimed television series set in a theme park called Westworld where "guests" (humans) interact with robots and play along in a storyline crafted by the Westworld corporation. The goal of the 'Westworld' corporation however is not merely to create an alternative world where guests can choose to pursue a second life; collecting data on guests is the core of Westworld's business model, and viewers and guests alike are oblivious as to what the corporation is using the data for.[3] In reality, many of the connected devices, or Internet of Things ("IoT") devices consumers use, collect data on consumers that is sometimes sold to third parties.[4] Like Westworld, the theme park is not really the product, the

[1] *See generally* Philip Bump, *Everything You Need to Know About the Cambridge Analytica-Facebook Debacle,* WASH. POST (Mar. 19, 2018), https://www.washingtonpost.com/news/politics/wp/2018/03/19/everything-you-need-to-know-about-the-cambridge-analytica-facebook-debacle/?utm_term=.894c89e1d3cb.

[2] *See* Kevin Fallon, *'Westworld' Season 2 Secrets Revealed: Facebook Data Collection, Badass Women and More,* DAILY BEAST (Apr. 20, 2018, 1:30 AM), https://www.thedailybeast.com/westworld-season-2-takes-on-facebook-data-collection-says-creator; *see also* Anna Menta, *'Westworld' Season 2 Premiere Hints At Facebook's Data Scandal,* NEWSWEEK (Apr. 22, 2018, 9:50 AM), https://www.newsweek.com/westworld-season-2-premiere-nods-facebook-data-scandal-889503.

[3] *See Westworld: Journey Into Night* (Home Box Office Apr. 22, 2018).

[4] *See* David Knight, *Who Owns the Data from the IoT?*, NETWORK WORLD (Jan. 30, 2017, 04:00 AM), https://www.networkworld.com/article/3152837/who-owns-the-data-from-the-iot.html; *see also* Jennifer Valentino-DeVries et al., *Your Apps Know Where You Were Last Night, and They're Not Keeping it Secret,* N.Y. TIMES (Dec. 10, 2018), https://www.nytimes.com/interactive/2018/12/10/business/location-data-privacy-apps.html (On mobile devices, data collected from apps are sold to third parties who "use or analyze the data to cater to advertisers, retail outlets and even hedge funds seeking insights into consumer behavior.").

*J.D. Candidate, Class of 2020, University of Illinois College of Law.

product is the consumer.[5] In many cases, this data is sold without the user's knowledge or informed consent.[6]

Such practices raise consumer privacy concerns, especially with the increasing security vulnerabilities associated with the connected devices consumers use such as connected cars, smart TVs, smart home devices, smart refrigerators, smart watches or fitness trackers, baby monitors, and pacemakers, to name a few.[7] These devices are classified as Internet of Things ("IoT") devices. The process by which consumer data is obtained from IoT devices has largely been unregulated in order to foster innovation in the tech industry.[8] The European Union, recognizing the security vulnerabilities of IoT devices, and the privacy concerns they raise, is now attempting to regulate IoT devices in the upcoming ePrivacy regulation.[9]

This Note argues that because of growing security and privacy issues associated with IoT devices, it is time for the United States to implement an IoT specific regulation similar to the ePrivacy Regulation. Part I is devoted to a brief discussion on what IoTs are, the breadth and scope of the upcoming ePrivacy regulation and how the ePrivacy regulation affects the IoT Industry. Part I also briefly discusses the current regulatory landscape in the United States. Further, Part II investigates why there is a need to regulate the Internet of Things Industry because of growing security and privacy issues. Finally, Part III puts forth recommendations for regulating the internet of things industry by the federal government or Federal Trade Commission (FTC).

II. BACKGROUND

A. What is Internet of Things?

The prominence of the internet has fueled inventors and tech companies to create products that connect consumers to technology, consumers to consumers, consumers to businesses, businesses to consumers, businesses to businesses, and businesses to technology.[10] Now, the

[5] *See* Danny Bradbury, *How Can Privacy Survive in the Era of the Internet of Things,* GUARDIAN (Apr. 7, 2015, 2:00 AM), https://www.theguardian.com/technology/2015/apr/07/how-can-privacy-survive-the-internet-of-things (Discussing how connected devices are inexpensive because the device is not really the product, the consumer is).

[6] *See* Valentino-DeVries, *supra* note 4 (According to the authors of the article, many of these privacy policies are often ambiguous. For example, "[a]n app may tell users that granting access to their location will help them get traffic information, but not mention that data will be shared and sold.").

[7] *See e.g.* Danny Palmer, *IoT Security Warning: Your Hacked Devices are Being Used for Cybercrime Says FBI*, ZDNET (Aug. 3, 2018, 6:17 AM), https://www.zdnet.com/article/iot-security-warning-your-hacked-devices-are-being-used-for-cyber-crime-says-fbi/; Lily Hay Newman, *An Elaborate Hack Shows How Much Damage IoT Bugs Can Do*, WIRED (Apr. 16, 2018, 1:00 PM), https://www.wired.com/story/elaborate-hack-shows-damage-iot-bugs-can-do/; Mayank Somani, *Connect the Dots: IoT Security Risks in an Increasingly Connected World*, SECURITY INTELLIGENCE (May 11, 2018), https://securityintelligence.com/connect-the-dots-iot-security-risks-in-an-increasingly-connected-world/.

[8] *See* Mauricio Paez & Keriabbe Tobit, *The Industrial Internet of Things: Risks, Liabilities, and Emerging Legal* Issues, 62 N.Y. L. SCH. L. REV. 217, 245 (2017) (The authors argue that one of the main reasons why there is no regulation of the IoT industry in the US is because regulators do not want to hinder the freedom tech companies have in making new products).

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

[10] *See generally, Internet of Things (IoT) History,* POSTSCAPES (Aug. 20, 2018), https://www.postscapes.com/internet-of-things-history/ (Providing a history of IoT products).

internet has helped power a new spell of connectivity that allows for connections between 'things.'[11] These 'things' refer to a wide variety of connected devices such as smart wearables (including smart watches, activity trackers and smart glasses), smart speakers, smart TVs, smart refrigerators, smart homes, smart cities, smart grids (smart metering) blood pressure monitoring devices, baby monitors, autonomous vehicles and many more.[12] This new stage of connectivity is sometimes called machine-to-machine (M2M)[13] communications.[14] There is currently no general definition for the term Internet of Things.[15] Nonetheless, the term usually refers to "the extension of network connectivity and computing capability to objects, devices, sensors, and items not ordinarily considered to be computers."[16] Computers and mobile devices are typically not categorized as IoT even though they are internet connected devices made up of sensors.[17]

The basic IoT system is not complex to understand. "A complete IoT system integrates four distinct components: sensors/devices, connectivity, data processing, and a user interface."[18] First, an IoT is embedded with sensors that "detect and capture data from the surrounding environment,[19] including the people who own the objects."[20] The captured and detected data is subsequently transmitted via satellite, WiFi or Bluetooth[21] to a cloud.[22] Finally, "that data is then analyzed for insights and intelligence that will guide decision making."[23] That is, once on the cloud the data is processed,[24] and the information obtained from the data is usually sent to an end-user if there is a display interface.[25] Where there is no display interface, the processed information performs functions automatically.[26]

[11] *See* Steven Weber & Richmond Y. Wong, *The New World of Data: Four Provocation on the Internet of Things,* PEER REVIEWED JOURNAL ON THE INTERNET (Feb. 6, 2017), available at, https://firstmonday.org/article/view/6936/5859.

[12] *See generally* Knud Lasse Lueth, *The 10 Most Popular Internet of Things Applications Right Now,* IOT ANALYTICS (Feb. 2, 2015), https://iot-analytics.com/10-internet-of-things-applications/.

[13] *See* Adam D. Thierer, *The Internet of Things and Wearable Technology: Addressing Privacy and Security Concerns without Derailing Innovation,* 21 RICH. J.L. & TECH 1, 7 (Calling IoTs "machine-to-machine connectivity and communications.").

[14] Some of the connected devices are controlled through an app on an end-user's phone. For example, in the smart home context, a smart home device like a thermostat is controlled from an app that is used to regulate temperature on an end-user's phone. *See* Swaroop Poudel, *Internet of Things: Underlying Technologies, Interoperability, and Threats to Privacy and Security,* 31 BERKELEY TECH. L.J. 997, 998 (2016).

[15] *See* Mauricio Paez & Mike La Marca, *The Internet of Things: Emerging Legal Issues for Business,* 43 N. KY. L. REV. 29, 31 (2016) (Stating that there is no "unified concept" for what internet of things are).

[16] KAREN ROSE ET. AL. INTERNET SOC'Y, THE INTERNET OF THINGS: AN OVERVIEW 12 (2015) *available at* https://www.internetsociety.org/wp-content/uploads/2017/08/ISOC-IoT-Overview-20151221-en.pdf; *see also* Paez & La Marca, *supra* note 15, at 31 (Defining IoT as "the growing number of everyday physical objects or 'things' that have been embedded with technology to enable them to interact with the physical environment, people, and other devices in real time.").

[17] Paez & La Marca, *supra* note 15, at 31.

[18] Calum McClelland, *IoT Explained – How Does an IoT System Actually Work?*, IOTFORALL (Nov. 20, 2017), https://medium.com/iotforall/iot-explained-how-does-an-iot-system-actually-work-e90e2c435fe7.

[19] Sensors that can detect changes in environment include: temperature sensors (like infrared sensors), proximity sensors (like ultrasonic sensors), pressure sensors, water quality sensors, chemical sensors, gas sensors, smoke sensors, level sensors, motion detection sensors, accelerometer sensors, gyroscope sensors, humidity sensors, optical sensors, and image sensors. Rita Sharma, *Top 15 Sensor Types Being Used in IoT,* FINOIT https://www.finoit.com/blog/top-15-sensor-types-used-iot/ (last visited Feb. 28, 2019).

[20] Paez & La Marca, *supra* note 15, at 31.

[21] McClelland, *supra* note 18.

[22] Paez & La Marca, *supra* note 15, at 31.

[23] *Id.*

[24] McClelland, *supra* note 18.

[25] *Id.*

[26] *See id.* (Stating that "rather than waiting for you to adjust the temperature, the system could do it automatically via predefined rules.").

IoTs promise to usher in the Fourth Industrial Revolution.[27] A 2018 study by Cisco estimates that IoT connections are expected to grow from 6.1 billion in 2017 to 14.6 billion by 2022,[28] with "1.8 M2M connections for each member of the global population by 2022."[29] In another study, Cisco also estimates that by 2020, there will 37 billion new connected devices on the market.[30] As more consumers continue to use IoTs, the economic impact of the devices will grow substantially. According to McKinsey Global Institute, IoTs could generate as much as $11.1 trillion a year by 2025.[31] These devices will "offer the potential for improved health-monitoring, safer highways, and more efficient home energy use, among other potential benefits."[32]

Businesses are also taking advantage of IoT systems.[33] Mauricio Paez and Kerianne Tobitsch maintain that the prevalence and rise of IoTs "has the promise to revolutionize the industrial sector in the United States and around the World."[34] They note that companies can use a network of IoTs composed of electronic sensors and industrial internet software among others, to analyze data that will help "guide decision-making, improve safety and organizational processes, reduce waste, promote efficiency, and lessen environmental impact."[35]

Despite the popularity of IoTs, many consumers are unaware the ability of IoTs to cache personal data, which raises privacy concerns[36] related to collecting data.[37] In some cases, the data retrieved by IoT companies can be used to formulate daily data journals of consumers and corporations.[38] Moreover, for many IoT device manufacturers, manufacturing secure devices

[27] *See* World Economic Forum, *The Fourth Industrial Revolution,* YOUTUBE (Apr. 13, 2016), https://www.youtube.com/watch?v=khjY5LWF3tg; *see also* Mark Torr, *Defining the Fourth Industrial Revolution: Where IoT Fits and the Potential,* MICROSOFT (Aug. 22, 2016), https://news.microsoft.com/europe/features/defining-the-fourth-industrial-revolution-where-iot-fits-and-the-potential/ (Agreeing with the World Economic Forum's labelling of IoTs as the Fourth Industrial Revolution because of their economic and sustainable benefits to the environment).

[28] *Cisco Visual Networking Index: Forecast and Trends, 2017–2022*, CISCO (Nov. 26, 2018), https://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/white-paper-c11-741490.html.

[29] *Id.*

[30] CISCO, THE INTERNET OF EVERYTHING AND THE CONNECTED ATHLETE: THIS CHANGES…EVERYTHING 2 (2013), *available at* https://www.cisco.com/c/en/us/solutions/collateral/service-provider/mobile-internet/white_paper_c11-711705.pdf.

[31] JAMES MANYIKA ET. AL., UNLOCKING THE POTENTIAL OF THE INTERNET OF THINGS 110 (McKinsey Global Institute June 2015), *available at* https://www.mckinsey.com/~/media/McKinsey/Business%20Functions/McKinsey%20Digital/Our%20Insights/The%20Internet%20of%20Things%20The%20value%20of%20digitizing%20the%20physical%20world/The-Internet-of-things-Mapping-the-value-beyond-the-hype.ashx.

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

[33] *See generally,* Insights Team, *Five Ways IoT is Reinventing Businesses Today,* FORBES (Aug. 24, 2018), https://www.forbes.com/sites/insights-inteliot/2018/08/24/5-ways-iot-is-reinventing-businesses-today/#216683b21c20.

[34] Paez & Tobit, *supra* note 8, at 218.

[35] *Id.* at 219.

[36] *See infra* section II.A.2 (Discussing privacy risks associated with IoT devices).

[37] *See Privacy and IoT: Innovative Regulation Needed to Regulate Innovation,* INTERNET OF BUS. (Dec. 2. 2016), https://internetofbusiness.com/privacy-iot-innovative-regulations/.

[38] *See* Susan Morrow, *Five Reasons Privacy and IoT Are Incompatible,* IOTFORALL (Oct. 26, 2018), https://www.iotforall.com/five-reasons-privacy-iot-incompatible/.

is an afterthought.[39] As a direct result, many of the IoT devices used by consumers are embedded with lower levels of security.[40]

B. The ePrivacy Regulation

In the EU, all citizens have a fundamental right to privacy.[41] Jane E. Kirtley and Scott Memmel note that compared to the US, "the EU prefers an omnibus approach to privacy through implementation of an overarching, blanket law regulating privacy consistently across industries, providing certain rights to EU citizens regardless of context."[42] The EU is currently in the process of implementing an overarching privacy and electronic regulation due in the second half of 2019[43] called the ePrivacy Regulation to join the already enacted General Data Protection Regulation (GDPR).[44] EU legislators intend for the ePrivacy regulation to keep up with advancements in a rapidly growing tech industry.[45] Before the regulation comes into force however, the ePrivacy Directive[46] still controls this area. Unlike a regulation, a directive requires countries in the EU bloc to implement provisions through local regulations.[47] This often leads to inconsistencies in enforcement.[48] Legislators in the EU felt that in order to ensure the protection of EU citizens' rights to privacy in an internet-based world, more stringent measures were needed.[49] Originally intended to be released in tandem with the General Data Protection Regulation (GDPR),[50] the ePrivacy regulation will become the second part of the EU's data protection reform framework.

The ePrivacy regulation is a communications data regulation.[51] The regulation is intended to apply telecommunication companies, internet service providers (ISPs) and companies that process personal data.[52] Whereas the GDPR regulates how data is protected, the new ePrivacy

[39] *See* Thor Olavsrud, *Security an Afterthought in Connected Home, Wearable Devices,* CIO (Sept. 8, 2016), https://www.cio.com/article/3117396/security-an-afterthought-in-connected-home-wearable-devices.html.

[40] *See* Andrew Tannenbaum, *Why Do IoT Companies Keep Building Devices with Huge Security Flaws?,* HARV. BUS. REV. (Apr. 27, 2017), https://hbr.org/2017/04/why-do-iot-companies-keep-building-devices-with-huge-security-flaws ("The problem is that many IoT devices are not designed or maintained with security as a priority.").

[41] *See* Charter of Fundamental Rights of the European Union, 2010 O.J. C 83/02, at 389 (Mar. 30, 2010).

[42] Jane E. Kirtley & Scott Memmel, *Rewriting the Book of the Machine: Regulatory and Liability Issues for the Internet of Things*, 19 MINN. J.L. SCI. & TECH. 455, 492 (2018).

[43] *See* Sandra Vogel & Dale Walker, *ePrivay Regulation: What is it and How Does it Affect me?,* ITPRO (Jan. 11, 2019), https://www.itpro.co.uk/privacy/32712/eprivacy-regulation-what-is-it-and-how-does-it-affect-me.

[44] *See* Commission Regulation 2016/679, 2016 O.J. (L 119) 1 (EU) [hereinafter GDPR] (Regulating the processing of data on EU citizens).

[45] *See ePrivacy Regulation, supra* note 9, at 10 (Stating that there is a need to regulate because "important technological and economic developments" have taken place over the last decade).

[46] *See* Council Directive 2002/58/EC, 2002 O.J. (L 201) (EC).

[47] *See* I-SCOOP, THE NEW EPRIVACY REGULATION: WHAT YOU NEED TO KNOW (i-scoop.eu), https://www.iscoop.eu/gdpr/eueprivacyregulation/#EU_ePrivacy_from_a_Directive_to_a_Regulation.

[48] *Id.*

[49] *ePrivacy Regulation, supra* note 9, at recital 1.1.

[50] *See* Natasha Singer, *The Next Privacy Battle in Europe Is Over This New Law,* N.Y. TIMES (May 27, 2018), https://www.nytimes.com/2018/05/27/technology/europe-eprivacy-regulation-battle.html (Stating that the reason why the ePrivacy regulation was not implemented in 2018 was because of internal disagreements).

[51] *See* Giovanni Buttarelli, *The Urgent Case for a New ePrivacy Law,* EUROPEAN DATA PROTECTION SUPERVISOR (Oct. 19, 2018), https://edps.europa.eu/press-publications/press-news/blog/urgent-case-new-eprivacy-law_en.

[52] *See* Kirtley & Memmel, *supra* note 42 at 499. It should be noted that when it comes to regulating companies that process data, the ePrivacy regulation is not unique in this task. One of the main goals of the GDPR is to regulate the processing of

regulation will regulate the privacy of communications.[53] It will "address[] in detail the confidentiality of electronic communications, and the tracking of internet users more broadly."[54] The new regulation will further prohibit the "listening, tapping, storing, monitoring, scanning or other kinds of interception, surveillance or processing of electronic communications data, persons other than the end-users,"[55] without an end-user's consent.[56]

Outside the context of IoTs, the ePrivacy regulation would apply to "Over-the-Top" (OTT) providers such as WhatsApp, Facebook, Gmail, Skype, iMessage and Netflix among others.[57] EU legislators also intend to police internet cookies to prevent unwarranted marketing by companies.[58] Further, citizens are afforded broad consent rights; specifically, the draft proposal states that end-users who have "consented to the processing of electronic communications data…shall be given the possibility to withdraw their consent at any time…and [they] must be reminded of this possibility at periodic intervals of 6 months, as long as the processing continues."[59]

Significantly, the provisions of the ePrivacy regulation will directly apply to M2M communications or IoTs. The draft regulation states that:

> In order to ensure full protection of the rights to privacy and confidentiality of communications, and to promote a trusted and secure *Internet of Things* in the digital single market, it is necessary to clarify that this Regulation should apply to the transmission of machine-to-machine communications. Therefore, the principle of confidentiality enshrined in this Regulation should also apply to the transmission of machine-to-machine communications.[60]

The scope of the regulation is broad and encompassing. Legislators intend for the regulation to apply to all companies that provide connected services or devices with end-users.[61] The provisions of the regulation will directly apply to any EU or non-EU company that provides electronic communication services to an EU citizen.[62] Just like the GDPR, the cost of noncompliance is substantial. Violating the provisions will mean fines of up to €10 million or 2% of a company's annual revenue, which ever one is higher.[63]

data. *See* Danny Palmer, *What is the GDPR? Everything you need to know about the new general data protection regulations,* ZDNET (May 23, 2018, 05:28 AM), https://www.zdnet.com/article/gdpr-an-executive-guide-to-what-you-need-to-know/

[53] Buttarelli, *supra* note 51.

[54] Natasha Lomas, *ePrivacy: An overview of Europe's other big privacy rule change,* TECH CRUNCH (Oct. 7, 2018), https://techcrunch.com/2018/10/07/eprivacy-an-overview-of-europes-other-big-privacy-rule-change/

[55] *ePrivacy Regulation, supra* note 9, at art. 5.

[56] *Id.* at art. 6.

[57] *Id.* at recital 1.1.

[58] *Id.* at recital 3.4–3.5

[59] *Id.* at art. 10.

[60] *Id.* at Proposal 12.

[61] This has been one of the major areas of contention with the regulation. Companies and even the United States Chamber of Commerce view this as "overly strict" and innovation stifling. *See* Singer*, supra* note 50.

[62] *ePrivacy Regulation, supra* note 9, at art. 3.

[63] *Id.* art. 23.

C. Current Regulatory Landscape in the United States

There is currently no overarching data privacy regulatory framework in the United States that polices data control or collection from IoT devices. Whereas the EU prefers an omnibus approach to protecting privacy, the United States prefers "a patchwork quilt of privacy laws that separately limit the use of Americans' medical records, credit reports…and so on."[64] But even with patchwork quilt privacy laws, data retrieved from IoT devices may not be covered. For example, healthcare data collected from fitness wearables like Fitbit or Apple Watch may not always fall under the Health Insurance Portability and Accountability Act (HIPAA) depending on who the data is shared with.[65] If the data from fitness wearables is shared with a healthcare provider or a doctor, that information is covered under HIPAA.[66] However, "HIPAA does not apply if the tech company does not share an end-user's health data with health-care providers,"[67] because manufacturers of fitness wearables are not defined as covered entities under HIPAA.[68] This means that fitness wearable manufacturers are free to utilize healthcare data retrieved from fitness wearables in any way they see fit, including sharing and selling of such data, provided such actions are listed in the terms and conditions of the fitness wearable's shrinkwrap agreement,[69] which consumers rarely read.[70]

The fact that HIPAA does not cover health data shared with third parties is no surprise given the FTC's self-regulatory approach to the IoT industry.[71] In lieu of having in place a robust regulatory framework, the FTC encourages IoT device manufacturers to follow "best business practices."[72] Some of these best practices include: security-by-design, privacy-by-design, notice and choice, security importance employee training, defense-in-depth strategies, and continuous device software updates to combat security risks.[73] However, the commission believes that Congress should look at implementing a substantive data security and breach notification law. Such calls have largely been disregarded by Congress.[74] On the state level,

[64] Natasha Singer, *Data Protection Laws, an Ocean Apart,* N.Y. TIMES (Feb. 2, 2013), https://www.nytimes.com/2013/02/03/technology/consumer-data-protection-laws-an-ocean-apart.html

[65] *See* Pamela Greenstone, *HIPAA guidelines should evolve with wearable technology,* THE HILL (Mar. 14, 2018 5:00PM), https://thehill.com/opinion/healthcare/378450-hipaa-guidelines-should-evolve-with-wearable-technology

[66] *See Id.*

[67] *Id.*

[68] *See* Nina Kostyukovsky, *Regulating Wearable Devices in the Healthcare Sector,* AMERICAN BAR (Sept. 27, 2018), https://www.americanbar.org/groups/health_law/publications/aba_health_esource/2014-2015/may/devices/

[69] *See* Kristen Lee, *Wearable health technology and HIPAA: What is and isn't covered,* SEARCH HEALTH IT, https://searchhealthit.techtarget.com/feature/Wearable-health-technology-and-HIPAA-What-is-and-isnt-covered (last visited Feb. 24, 2019)

[70] *See generally, See* Tess Wilkinson-Ryan, *A Psychological Account of Consent of Fine Print*, 99 IOWA L. REV. 1745 (2014) (Providing an in-depth analysis on a general reading problem related to modern consumer contracting).

[71] *See generally* FED. TRADE COMM'N, FTC STAFF REPORT: INTERNET OF THINGS: PRIVACY & SECURITY IN A CONNECTED WORLD, 48 (Jan. 2015) [hereinafter FTC IOT REPORT], https://www.ftc.gov/system/files/documents/advocacy_documents/comment-staff-federal-trade-commissions-bureau-consumer-protection-consumer-product-safety/p185404_ftc_staff_comment_to_the_consumer_product_safety_commission.pdf

[72] *See* FTC Report Press Release, *supra* note 32.

[73] *Id.*

[74] Although there is no substantive data security regulation, there have been two bills so far that have attempted to regulate some IoT. The first is a 2017 bill introduced by U.S. Senators Warner, Gardner, Wyden and Daines that attempts to improve cybersecurity of IoT devices bought by the government. The other is a bill introduced by former Michigan Rep. David Trott, called the "Internet of Medical Things Resilience Partnership Act of 2017, aimed at increasing the security and resilience of Internet of Medical Things devices." *See* Kirtley & Memmel, *supra* note 42 at 472–73.

California is the only state to have passed an IoT specific legislation aimed at ensuring that IoT devices are secure to prevent hacks and surveillance by cybercriminals.[75]

III. Analysis

In a world of constant data breaches,[76] there needs to be greater attention devoted to regulating the IoT industry. Some analysts even believe that the worst has yet to happen.[77] In the tech industry, companies view any approach to regulate as an approach that restricts their innovative freedom and hinders their ability to drive up profits. On that matter, the FTC seems to agree with the tech industry. The commission's laissez faire, self-regulatory approach to IoT device manufactures as a way of combatting consumer privacy and security risks is clearly one that is geared towards protecting commerce rather than consumers. Jan Philipp Albrecht, a European Union legislator who worked on draft regulations for the GDPR, noted that in his view, "the U.S. Chamber of Commerce and Commerce Department are mostly just following the interest of Silicon Valley."[78] The transaction costs involved with self-regulation makes it even harder for such a policy to work, "because the responsibility of IoT privacy and security falls upon several actors in the IoT industry, including manufacturers, network providers, software developers, and others, [thus,] it is difficult for the industry to develop industry-wide standards."[79]

Consumers for their part do not think that the current self-regulatory approach protects their privacy. A study by Axios found that 83% of consumers want stricter regulations and more stringent sanctions for privacy breaches, while 67% also support implementing a regulation similar to the GDPR.[80] These results are perhaps born out of the increasing security and privacy risks associated with many IoT devices.

1. Security Risks and Vulnerabilities

Security vulnerabilities of IoT devices presents one of the primary reasons why there needs to be an IoT specific regulation. Because IoT devices are connected to the internet, they are as vulnerable to cyber-attacks[81] as traditional computers, however, with IoT devices, this vulnerability is especially heightened.[82] In fact, the current IoT security vulnerabilities is

[75] *See* Adi Robertson, *California just became the first state with an Internet of Things cybersecurity law*, THE VERGE (Sept. 28, 2018), https://www.theverge.com/2018/9/28/17874768/california-iot-smart-device-cybersecurity-bill-sb-327-signed-law

[76] *See generally* Mike Snider, *Your data was probably stolen in cyberattack in 2018 – and you should care,* USA TODAY (Dec. 28, 2018), https://www.usatoday.com/story/money/2018/12/28/data-breaches-2018-billions-hit-growing-number-cyberattacks/2413411002/; *See also* Andrew Colley, *More that 80 percent of companies hit with IoT breaches,* CSO (Mar. 1, 2017), https://www.cso.com.au/article/615124/more-than-80-per-cent-companies-hit-iot-breaches-study/

[77] *See generally* Sooraj Shar, *Serious IoT data breach likely by 2020, say risk professionals,* INTERNET OF BUS. (Mar. 26, 2018), https://internetofbusiness.com/iot-data-breach-third-party/

[78] Singer, *supra* note 50.

[79] Kirtley & Memmel, *supra* note 42 at 471.

[80] *See* Kim Hart, *Americans Don't trust tech companies on data privacy,* AXIOS (Apr. 23, 2019), https://www.axios.com/distrust-social-media-firms-to-protect-privacy-survey-8b95db51-f137-46e3-a239-a5f304f0ac1b.html

[81] *See* Kirtley & Memmel, *supra* note 42 at 460.

[82] *See* FTC IoT Report, *supra* note 71, at 10.

similar to security vulnerabilities of computer devices in the early days of the internet[83] where "companies all over the world rushed haphazardly into the internet 'gold rush' without adequately addressing internet security. Viruses, worms, and spam subsequently descended on users. In many ways history may be repeating itself with IoT."[84] But, unlike computer systems that are frequently updated with patches to reduce and prevent cyberattacks, "many IoT devices have not been designed to use such patches in their software, leaving security issues unresolved."[85]

This IoT software security vulnerability stems from the inadequate firmware used in manufacturing some connected devices.[86] Because "embedding adequate levels of security into IoT devices would cost more, require specialized expertise, and may even involve product redesigns to accommodate different types of processors that power the security features,"[87] businesses and consumers are disadvantaged with IoT devices that are insecure.[88] A 2017 survey conducted by Altman Vilandrie & Company found that of approximately 400 IoT companies across 19 industries, 48% have experienced a data breach.[89] HP also conducted a survey in 2014 that found that there were around 25 security flaws associated with an average IoT device.[90] More worryingly, another study conducted by IBM and the Ponemon Institute found that "80% of organizations do not routinely test their IoT apps for security vulnerabilities."[91]

The FTC recognizes the security concerns associated with IoT devices. The commission noted in its 2015 report that security risks inherent in IoT devices "could be exploited to harm consumers by: (1) enabling unauthorized access and misuse of personal information; (2) facilitating attacks on other systems; and (3) creating safety risks."[92] Since that report was published consumers and businesses have been left to bear the burden of security flaws caused by insecure firmware associated with IoT devices. In 2016, IoTs and the internet in general, experienced the largest cyber-attack in history facilitated by a malware called Mirai Botnet,[93]

[83] *See generally,* Craig Timberg, *The real story of how the internet became so vulnerable,* WASH. POST, (May 30, 2015), https://www.washingtonpost.com/sf/business/2015/05/30/net-of-insecurity-part-1/?noredirect=on&utm_term=.99d79ab9bba5

[84] Matt Toomey, *IoT Device Security is Being Seriously Neglected,* ABERDEEN (Feb. 5, 2018), https://www.aberdeen.com/techpro-essentials/iot-device-security-seriously-neglected/

[85] Kirtley & Memmel, *supra* note 42 at 461. Nick Ismail of Information Age gives a good summary of this problem: "Consider the operating systems for such [devices]. How do you upgrade the OS in a wall-mounted air conditioning unit that's connected wirelessly? Or a smart light bulb? If you can't upgrade an operating system, how can you attempt to patch any vulnerabilities?" Nick Ismail, *The Internet of Things: The security crisis of 2018?* INFORMATION AGE (Jan. 22, 2018), https://www.information-age.com/internet-things-security-crisis-123470475/

[86] *See* Toomey, *supra* note 84.

[87] *Id.*

[88] *See* Gary Eastwood, *4 critical security challenges facing IoT,* NETWORK WORLD (Feb. 7, 2017, 4:39AM), https://www.networkworld.com/article/3166106/internet-of-things/4-critical-security-challenges-facing-iot.html

[89] *See Survey: Nearly Half of U.S. Firms Using Internet of Things Hit By Security Breaches,* BUS. WIRE, (June 1, 2017, 11:36AM), https://www.businesswire.com/news/home/20170601006165/en/Survey-U.S.-Firms-Internet-Things-Hit-Security

[90] *See,* Matthew Sparkes, *Average Internet of Things device has 25 security flaws,* THE TELEGRAPH (July 30, 2014, 11:26AM) https://www.telegraph.co.uk/technology/internet-security/11000013/Average-Internet-of-Things-device-has-25-security-flaws.html

[91] Tannenbaum, *supra* note 40.

[92] FTC IOT REPORT, *supra* note 71, at 10.

[93] *See generally* Josh Fruhlinger, *CCTV cameras almost brought down the internet,* CSO (Mar. 9, 2018, 3:00AM), https://www.csoonline.com/article/3258748/security/the-mirai-botnet-explained-how-teen-scammers-and-cctv-cameras-almost-brought-down-the-internet.html

which caused much of the internet to go down in the United States.[94] The perpetrators exploited insecure firmware flaws in IoT devices to pull off this attack.[95] The attack was successfully orchestrated by using mirai infected computers to "continually search the internet for vulnerable IoT devices and then use known default usernames and passwords to log in, infecting [the IoTs] with malware."[96] Outside the U.S., a more alarming scenario presented itself with a hack on a smart electronic key system at a hotel in Austria "locking guests out of their rooms until the hotel paid ransom."[97] Hackers were able to compromise the key system because of inadequate security design and maintenance.[98] In the business setting, researchers at Senrio, an IoT-focused security firm, detailed how easy it is for hackers to hack into a business through weak IoT devices like security cameras as a pathway to access other company networks.[99] In the staged attack, researchers used a software tool to scan for vulnerable unpatched company security cameras "sitting on the public internet."[100] Such compromised security cameras can be used as an entry point to attack routers, allowing hackers to easily gain access to valuable company data.[101]

Despite the prevalence of these security risks and malware attacks, in 2017, a former FTC acting commissioner stated that she wanted IoT companies to continue to formulate best industry practices among themselves.[102] This statement is problematic given IoT manufacturers lax approach to solving security flaws in the face of increased malware attacks. As Bruce Schneier, Fellow and Lecturer at Harvard Kennedy School of Government puts it, "the market is not going to provide security on its own, because there is no incentive for buyers or sellers to act in anything but their self-interest."[103] IoT manufacturers will not take device security seriously unless a regulatory framework is in place.[104]

2. *Privacy Risks*

Unlike security flaws that may be resolved through technical solutions for ensuring data is protected outside regulations, IoT privacy issues cannot seriously be tackled outside regulations.[105] So far, the FTC's market approach has failed to ensure consumer privacy is protected. Companies are more concerned about their bottom dollar and the race to put new

[94] *See* Nicky Woolf, *DDoS attack that disrupted internet was largest of its kind in history, experts say,* GUARDIAN (Oct. 26, 2016, 4:42PM), https://www.theguardian.com/technology/2016/oct/26/ddos-attack-dyn-mirai-botnet (Stating that the attack caused websites like Twitter, the Guardian, Netflix, Reddit and CNN to go down).

[95] *See The 5 Worst Examples of IoT Hacking and Vulnerabilities in Recorded History,* IOTFORALL, (May 10, 2017), https://www.iotforall.com/5-worst-iot-hacking-vulnerabilities/ [hereinafter *IoT Hacking and Vulnerabilities*]

[96] *Id.*

[97] Tannenbaum, *supra* note 40.

[98] *Id.*

[99] *See* Newman, *supra* note 7.

[100] *Id.*

[101] *Id.*

[102] *See* Sam Thielman, *Acting Federal Trade Commission head: internet of things should self-regulate,* GUARDIAN (Mar. 14, 2017, 6:00AM), https://www.theguardian.com/technology/2017/mar/14/federal-trade-commission-internet-things-regulation

[103] Press Release, Senators Introduce Bipartisan Legislation to Improve Cybersecurity of "Internet-of-Things" (IoT) Devices, (Aug. 1, 2017) [hereinafter Senate IoT Bill], https://www.warner.senate.gov/public/index.cfm/2017/8/senators-introduce-bipartisan-legislation-to-improve-cybersecurity-of-internet-of-things-iot-devices

[104] *See* Toomey, *supra* note 84.

[105] *See* Bryon Meyer, *Policy and Regulation in the IoT World: Should There Be Structure?*, ELECTRONIC ENGINEERING JOURNAL (Feb. 19, 2018) https://www.eejournal.com/article/policy-and-regulations-in-the-iot-world/.

products on the market that will become the next big thing. In fact, privacy rarely gets the much-needed attention it deserves by tech companies.[106] Data maximization seems to be the norm for companies in the tech industry where the practice is "keep the information until you run out of server space."[107] These companies are free to use the information they keep in any way they want, increasing concerns about misuse of sensitive consumer personal data.

The FTC is keenly aware of the risks posed by the data maximization practices of IoT companies. In a 2015 report,[108] the FTC noted that many IoTs devices collect sensitive personal information including consumer habits, physical conditions, health information, detailed geolocation, and financial account numbers,[109] all of which can be easily compromised given the major security risks posed by IoT devices.[110] This type of data harvesting, even in cases where consumers consent, can be used to create detailed and extensive data journals of consumers.[111] Absent a robust regulatory framework that polices the data maximization practices of IoT companies, sensitive behavioral patterns of consumers may be sold to other companies who may use the data obtained for insurance, credit, and employment decisions, among others.[112] What if, for example, car sensors that warn drivers about bad driving habits are used to deny consumers car insurance based on the data journals retrieved and sold to interested parties?[113] What if data retrieved from a consumer's Apple Watch is transmitted to your health insurance provider who uses it in insurance decision-making?[114] Perhaps, these questions and many more factored into decisions by EU legislators when deciding to regulate IoTs.

In addition, the ubiquity of IoT devices raises concerns about electronic surveillance. Because of the physical configuration of IoT devices (e.g. smart speakers, some smart wearables, smart toys, smart baby monitors)[115] consumers are sometimes unaware that they are being tracked or listened to because "conveying or updating a privacy policy or consenting to terms of service is not easily possible without a screen."[116] There have been instances where consumers have caught their Amazon Echo devices listening in on their conversations without engaging the devices' Alexa voice assistant.[117] In other instances, smart toys have been known

[106] *See* Rob Pegoraro, *Big tech firms still don't care about your privacy,* WASH. POST (Jan. 28, 2019), https://www.washingtonpost.com/outlook/2019/01/28/big-tech-firms-still-dont-care-about-your-privacy/?utm_term=.aee1b646a752 (Pointing out the simple steps that tech companies can take to protect privacy that they are currently neglecting).

[107] *Id.*

[108] FTC IOT REPORT, *supra* note 71, at 14–18.

[109] *Id.* at 14.

[110] *See Infra* section II.A.1 (Discussing security risks posed by IoT devices)

[111] *See* FTC IOT REPORT, *supra* note 71, at 15. (For example, the report noted that "researchers are beginning to show that existing smartphone sensors can be used to infer a user's mood; stress levels; personality type; bipolar disorder; demographics…smoking habits; overall well-being; progression of Parkinson's disease; sleep patterns; happiness; level of exercise; and types of physical activity or movement").

[112] *Id.* at 16.

[113] *See* Bradbury, *supra* note 5.

[114] *See* FTC IOT REPORT, *supra* note 71, at 15-16 (Recognizing the risks posed by data journals retrieved from wearable fitness trackers).

[115] *See* Laura DeNardis & Mark Raymond, *The Internet of Things as a Global Policy Frontier,* 51 U.C.D.L. REV. 475, 483 (2017)

[116] *Id.*

[117] *See e.g.* Niraj Chokshi, *Is Alexa Listening? Amazon Echo Sent Out Recording of Couple's Conversation,* N.Y. TIMES (Mar. 25, 2018), https://www.nytimes.com/2018/05/25/business/amazon-alexa-conversation-shared-echo.html; Will Oremus, *Terrifyingly Convenienty*, SLATE (Apr. 3, 2016, 8:04PM)

to listen in on conversations,[118] even prompting the FBI to release a report[119] warning consumers the security risks associated with some smart toys.

Relatedly, if IoT devices like the Amazon Echo can listen in on conversations, how long will it take before cyber criminals take advantage of security vulnerabilities inherent in some devices allowing them to eavesdrop on the private lives of consumers? Again, what if law enforcement agencies are able to tap IoT devices "leading to warrantless surveillance or illegal searches and recordings in violation of common law, privacy, and Fourth Amendment rights[?]"[120] As Laura DeNardis and Mark Raymond note "the private data collection of everyday objects and activities heightens opportunities for government surveillance of . . . everyday activities, whether for law enforcement, domestic or foreign intelligence gathering, or politically motivated tracking of dissidents and media."[121]

Some courts seem to be embracing the fact that devices like the Amazon Echo listen in on conversations. For example, a Judge in New Hampshire demanded Amazon hand over audio recordings that may help solve a murder case.[122] This raises questions about just how much information IoT devices retrieve, and how easy it may be for law enforcement agencies to gain access to consumer data that consumers had no knowledge was being collected. So where will the margin be drawn? "Will data be used for just violent crimes, or will law enforcement eventually want to pore over data for parking violations and minor misdemeanors?"[123]

There are more questions than answers, and without a robust framework that is geared towards targeting privacy risks associated with IoT devices, the widespread use of these connected devices may herald in a new era where an individual's privacy expectation is nothing but a relic. "Left unchecked, IoT devices could allow intrusive surveillance into the private spheres of individuals' lives."[124]

IV. Recommendations

Proponents of having no regulation of the IoT devices have raised concerns with EU legislators[125] that any regulation will lead to less innovation in the tech industry. Some have argued "that freedom to harvest personal data is needed in order to develop new technologies, such as artificial intelligence tools."[126] Others have argued that the regulation will make it too

http://www.slate.com/articles/technology/cover_story/2016/04/alexa_cortana_and_siri_aren_t_novelties_anymore_they_re_our_terrifyingly.html.

[118] *See* Elisabeth Leamy, *The Danger of giving your child 'smart'toys,* WASH. POST (Sept. 29, 2017), https://www.washingtonpost.com/lifestyle/on-parenting/giving-your-child-internet-connected-smart-toys-could-be-dumb/2017/09/29/a168218a-a241-11e7-8cfe-d5b912fabc99_story.html?utm_term=.9785bec5b592

[119] *See Consumer Notice: Internet-Connected Toys Could Present Privacy and Contact Concerns for Children,* FBI (July 17, 2017), https://www.ic3.gov/media/2017/170717.aspx

[120] Kirtley & Memmel, *supra* note 42, at 466.

[121] DeNardis & Raymond, *supra* note 115, at 482.

[122] *See* Chavie Lieber, *Amazon's Alexa Might be a key witness in a murder case,* VOX (Nov. 12, 2018 5:00 PM), https://www.vox.com/the-goods/2018/11/12/18089090/amazon-echo-alexa-smart-speaker-privacy-data

[123] *Id.*

[124] Poudel, *supra note* 14, at 1013.

[125] *See* David Meyer, *Inside the ePrivacy Regulation's furious Lobbying war,* IAPP: PRIVACY ADVISOR, (Oct. 17, 2017), https://iapp.org/news/a/inside-the-eprivacy-regulations-furious-lobbying-war/ (European Legislator, Jan Philipp Albrecht noted that the tech industry has been engaged in a massive lobbying, with some in the industry going as far to say that the ePrivacy regulation will be the death of apps and free services online).

[126] Buttarelli, *supra* note 51.

costly for IoT manufacturers to produce new products.[127] But the security[128] and privacy risks[129] pointed out in this Note, highlight the need for an IoT specific regulation. Despite FTC recommendations,[130] IoT devices continue to be attacked by hackers. Without a robust mandatory regulatory framework, IoT manufacturers will not prioritize security and consumer privacy.

Moreover, the inherent lack of transparency of the data maximization practices of many firms in the tech industry amplifies the need for regulation.[131] Will it truly hurt companies to tell consumers if and when their data is being collected and what their data is being collected for? In most cases this will give companies the opportunity to develop consumer trust and openness. Surveys show that consumers are worried about privacy[132] and will take their business elsewhere if companies do not take security concerns seriously. For example, a survey conducted by PricewaterhouseCoopers (PWC) found that 85% of consumers will stop doing business with companies "if they have concerns about its security practices."[133] IoT device manufacturers should be cognizant of consumer perceptions and welcome an IoT specific regulation as a chance to develop trust and openness with consumers.

In the event that federal regulators decide to formulate an IoT specific regulation they should consider four key provisions as part of any regulatory framework: (1) Security by design and default, (2) Privacy by design and default, (3) Data Breach Notification, and (4) Sanctions.

1. *Security by Design and Default*

Security by design and default should be required for all IoT devices. This will require security to be embedded into every IoT device at the outset. Regulators should start at targeting security issues at the engineering level. This must include requiring IoT devices to have a minimum level of security. Here regulators can use the Senate bill authored by U.S. Senators Warner, Gardner, Wyden and Daines as a starting point in formulating a framework for all IoT devices on the market, and not just IoT devices purchased by the government.[134] The bill required IoT manufacturers to ensure that government purchased IoT devices are "patchable, do not include hard-coded passwords that can't be changed, and are free of known security

[127] *See* Bruce Gustafson, *Economic Impact of the prosed European ePrivacy Regulation,* DEVELOPERS ALLIANCE, (May 25, 2018), *available at,* https://webcache.googleusercontent.com/search?q=cache:7BV9IPTp0xMJ:https://www.orange.com/en/content/download/46903/1368006/version/2/file/Economic%252Bimpacts%252Bof%252Bthe%252Bproposed%252BEuropean%252BePrivacy%252BRegulation.pdf+&cd=9&hl=en&ct=clnk&gl=us&client=safari

[128] *See infra* section II.A.1.

[129] *See infra* section II.A.2.

[130] *See* FTC IOT REPORT, *supra* note 71, at 10.

[131] *See* Valentino-DeVries et al., *supra* note 4.

[132] For example, a survey conducted by Park associates on consumers who use smart home technologies found that "88% feel negatively about companies using their personal data to figure out when they are likely to be home." *See* Nicholas Shields, *New aurvey shows consumers are wary of smart devices invading their privacy,* BUS. INSIDER (Apr. 26, 2018), https://www.businessinsider.com/survey-says-consumers-have-privacy-concerns-with-smart-home-devices-2018-4

[133] PRICEWATERHOUSECOOPERS, CONSUMER INTELLIGENCE SERIES: PROTECT.ME, (2017), https://www.pwc.com/us/en/advisory-services/publications/consumer-intelligence-series/protect-me/cis-protect-me-findings.pdf

[134] *See* Senate IoT Bill, *supra* note 103.

vulnerabilities."[135] Patching presents the biggest security vulnerability with IoT devices.[136] Regulators should look at requiring IoT devices to have built-in firmware that allows devices to be patched to ensure that software is frequently updated to prevent future cyber-attacks.

Elimination of hard-coded passwords that are set at the factory stage will also help curb security concerns.[137] Regulators should ensure IoT manufacturers design products that allow consumers to change factory set passwords.[138] In the event that certain IoT devices do not allow consumers to change factory default passwords, regulators should require IoT manufacturers to set passwords that are uniquely identifiable to the manufacturer. Giving consumers the opportunity to change passwords or requiring device manufacturers to use unique password credentials will further help alleviate security issues related to insecure web interface, insecure cloud interface, insecure mobile interface, and insufficient authentication.[139] The Mirai botnet attack[140] for example was made possible because the system of IoT devices hacked could not be patched because of existing firmware issues,[141] along with easily identifiable default passwords that were known to the hackers.[142]

2. *Privacy by Design and Default*

Like security by design and default, regulators must ensure that privacy is embedded at every stage of the data collection, data storage, and data sharing process. Data minimization and not maximization should be required for all companies in the IoT industry. This will mean implementing a provision similar to article 5 of the draft proposal of the ePrivacy regulation that prohibits "listening, tapping, storing, monitoring, scanning or other kinds of interception, surveillance or processing of electronic communications data, persons other than the end-users" without an end-user's consent.[143] If a consumer consents, federal regulators should consider requiring IoT device manufacturers share consumer data journals with the consumer periodically, as well as allowing consumers the opportunity to have their data erased if collection practices are being used outside the purpose for which consent was giving.[144] Consumers should further be afforded broader consent rights and must be given the opportunity to retract their consent periodically if they do not consent to the data collection or data sharing practices of IoT device manufacturers.[145] Finally, it is also imperative that regulators clarify whether data journals of consumers retrieved from IoT devices can be obtained by courts and law enforcement without the consumer's consent.

[135] *Id.*

[136] *See* Xu Zou, *IoT devices are hard to patch: Here's why – and how to deal with security,* TECH BEACON, https://techbeacon.com/security/iot-devices-are-hard-patch-heres-why-how-deal-security (last visited Feb. 14, 2019).

[137] *See* Tannenbaum, *supra* note 40 (Stating that "many IoT devices share default user names and passwords that are well known and can be found with a quick Google search").

[138] *Id.*

[139] *See* Ashwin Pal, *The Internet of Things (IoT) – Threats and Countermeasures,* CSO, https://www.cso.com.au/article/575407/internet-things-iot-threats-countermeasures/ (last visited Feb. 18, 2019).

[140] *See infra* section II.A.1.

[141] Fruhlinger*, supra* note 93.

[142] *IoT Hacking and Vulnerabilities*, *supra* note 95.

[143] *ePrivacy Regulation, supra* note 9, at art. 5.

[144] GDPR, *supra* note 44, at art 17.

[145] *ePrivacy Regulation, supra* note 9, at art. 10.

3. *Data Breach Notification*

To ensure transparency and trust with consumers and government officials, federal regulators should consider data breach notification requirements to both federal regulators and consumers. Regulators should require that IoT device manufacturers implement data breach notification protocols, similar to standards set by the EU in the GDPR.[146] For example, in the event of a data breach, companies are required to notify EU regulators within 72 hours of a data breach,[147] and must describe the gravity of the data breach,[148] names and contacts of consumers affected,[149] the consequence of the data breach,[150] and the measures taken to mitigate the effects of the data breach.[151] Since many of the IoT device manufacturers do business in the EU, it is possible that most of them already have systems in place to fall in compliance with the GDPR. Federal regulators should look into extending similar protocols to IoT companies who do business with American consumers.

4. *Sanctions*

To ensure full compliance with security and privacy safeguards, any regulation must consider levying administrative sanctions or fines. Here, regulators should look to other jurisdictions around the world that have data protection and privacy regulations to formulate sanctions that are necessary to ensure full compliance. For example, in France, sanctions include formal notices, warnings, injunctions and fines (under local laws and GDPR).[152] Across the EU, under the GDPR and ePrivacy regulations, failure to comply with the provisions of the regulations may lead to fines of €20 million or 4% of a company's annual revenue[153] and €10 million or 2% of a company's annual revenue respectively.[154]

V. Conclusion

It is time for federal regulators and the FTC to rethink self-regulation of IoT device manufacturers. In the FTC's 2015 report on the privacy and security concerns in a connected world, the FTC staff stated that, they do "not believe that the privacy and security risks, though real, need to be address through IoT-specific legislation at this time."[155] It has now been four years since that report was released. Since then, there has been an increase in IoT malware attacks that have compromised consumer security and privacy. Now more than ever, is the time for federal legislators to formulate a regulatory framework designed to police the IoT industry.

[146] *See* GDPR, *supra* note 44, at art. 33.

[147] *See Id.* at art. 33(1).

[148] *See Id.* at art. 33(1)(a).

[149] *See Id* at art. 33(1)(b).

[150] *See Id* at art. 33(1)(c).

[151] *See Id* at art. 33(1)(d).

[152] *See* Danhoe Reddy-Girard, *French Data Protection Rules,* 46 INT'L L. NEWS 11, 13–14 (2017).

[153] GDPR, *supra* note 44, at art. 83.

[154] *ePrivacy Regulation, supra* note 9, at art. 3.

[155] FTC IOT REPORT, *supra* note 71, at 48.