Fordham Intellectual Property, Media and Entertainment Law Journal

Volume 28 *XXVIII*
Number 1

Article 2

2017

After the Gold Rush: The Boom of the Internet of Things, and the Busts of Data-Security and Privacy

Dalmacio V. Posadas Jr.
Judicial Law Clerk, Central District of California, Dalmaciop@gmail.com

After the Gold Rush: The Boom of the Internet of Things, and the Busts of Data-Security and Privacy

Cover Page Footnote

Dalmacio V. Posadas, Jr. graduated from Loyola Law School, Los Angeles in 2017, and is a judicial law clerk in the Central District of California. The Author would like to give special thanks to Professors John Nockleby and Karl Manheim. The Author would also like to thank his wife Michelle Horejs, as well as Sonny and Dexter for their support.

After the Gold Rush: The Boom of the Internet of Things, and the Busts of Data-Security and Privacy

Dalmacio V. Posadas, Jr.*

This Article addresses the impact that the lack of oversight of the Internet of Things has on digital privacy. While the Internet of Things is but one vehicle for technological innovation, it has created a broad glimpse into domestic life, thus triggering several privacy issues that the law is attempting to keep pace with. What the Internet of Things can reveal is beyond the control of the individual, as it collects information about every practical aspect of an individual's life, and provides essentially unfettered access into the mind of its users. This Article proposes that the federal government and the state governments bend toward consumer protection while creating a cogent and predictable body of law surrounding the Internet of Things. Through privacy-by-design or self-help, it is imperative that the Internet of Things—and any of its unforeseen progeny—develop with an eye toward safeguarding individual privacy while allowing technological development.

* Dalmacio V. Posadas, Jr. graduated from Loyola Law School, Los Angeles in 2017, and is a judicial law clerk in the Central District of California. The Author would like to give special thanks to Professors John Nockleby and Karl Manheim. The Author would also like to thank his wife Michelle Horejs, as well as Sonny and Dexter for their support.

INTRODUCTION

> "Because, you know, resilience—if you think of it in terms of the Gold Rush, then you'd be pretty depressed right now because the last nugget of gold would be gone. But the good thing is, with innovation, there isn't a last nugget. Every new thing creates two new questions and two new opportunities." – Jeff Bezos[1]

In 1969, in an attempt to send the first electronic transmission through an early-model computer, University of California, Los Angeles students attempted to type in the word "login" but the computer crashed after typing in the second letter.[2] Tim Berners-Lee would soon after develop what we know today as the Internet.[3] Less than fifty years later, electronic transmissions are capable of complex and high-speed communication. Amidst the development of the Internet, the legal system has attempted to keep pace with the ever-growing and dynamic nature of the technological boom. All things Internet and electronic have provided a boon to society while also complicating related legal issues. In the relatively short life of the Internet, the legal system has attempted to adapt and address new privacy concerns such as: personal computers in the 1980s; the Internet in the 1990s; mobile apps at the beginning of the 2000s; and currently, the Internet of Things ("IoT"),[4] with

---

[1] Jeff Bezos, Founder & CEO, Amazon.com, Address at the TED2003 Conference: The Electricity Metaphor for the Web's Future (Feb. 2003), https://www.ted.com/talks/jeff_bezos_on_the_next_web_innovation/transcript?language=en [https://perma.cc/CG2W-NN6Y].

[2] *See* Daily Mail Reporter, *Pictured: The Fridge-Sized Computer that Sent the Very First Email [Fourty] Years Ago . . . But Crashed After Just Two Letters Were Received*, DAILY MAIL (Nov. 1, 2009), http://www.dailymail.co.uk/sciencetech/article-1224100/Internets-40th-birthday-First-email-crashes-just-letters.html [https://perma.cc/SQ2K-H4RG].

[3] *See* TIM BERNERS-LEE, WEAVING THE WEB: THE ORIGINAL DESIGN AND ULTIMATE DESTINY OF THE WORLD WIDE WEB BY ITS INVENTOR 2–3 (1999).

[4] *See* Stephen Lawson, *Look Before You Leap: [Four] Hard Truths About IoT*, PCWORLD (Mar. 23, 2017, 5:00 AM), http://www.pcworld.com/article/3184327/internet-of-things/look-before-you-leap-4-hard-truths-about-iot.html [https://perma.cc/QBK5-UL2M]; *see also* Maureen Dowd, *Elon Musk's Billion-Dollar Crusade to Stop the A.I. Apocalypse*, VANITY FAIR (Apr. 2017), http://www.vanityfair.com/news/2017/03/elon-musk-billion-dollar-crusade-to-stop-ai-space-x?utm_source=newsletter&utm_medium=email&utm_campaign=newsletter_axiosam [https://perma.cc/4K82-2RLX] ("'Your

artificial intelligence ("AI") hot on its heels.[5] Nevertheless, as technology evolves into the vast and unknown, IoT, data-security, and privacy issues remain. And in the IoT, these privacy issues are exacerbated because of the blurred lines between digital and physical infrastructures.[6]

What the IoT can reveal is beyond the control of the individual, as it collects information about every practical aspect of an individual's life, and provides essentially unfettered access into the mind of its user.[7] In their seminal work on privacy, Samuel Warren and Justice Brandeis determined that the right to privacy was the "right to be let alone."[8] The right to privacy was essentially the right to control your own personal information.[9] In a recent survey

---

phone and your computer are extensions of you, but the interface is through finger movements or speech, which are very slow.' With a neural lace inside your skull you would flash data from your brain, wirelessly, to your digital devices or to virtually unlimited computing power in the cloud. 'For a meaningful partial-brain interface, I think we're roughly four or five years away.'" (quoting Elon Musk CEO and founder of SpaceX, CEO and co-founder of Tesla, CEO and founder of Neuralink, and co-Chairman of OpenAI)). Perhaps in the near future AI will guide the digital privacy debate.

5 *See* Joseph Jerome, *Why Artificial Intelligence May Be the Next Big Privacy Trend*, IAPP (Oct. 10, 2016), https://iapp.org/news/a/why-artificial-intelligence-may-be-the-next-big-privacy-trend/ [https://perma.cc/5TUB-D6TU].

6 *See* Lawson, *supra* note 4 ("[A] Technalysis survey last year found operations departments were in charge of IoT projects more often than IT shops." (citation omitted)).

7 Despite Chief Justice Roberts's sardonic riff on the state of legal scholarship, Kant may be an appropriate—if not highly relevant—entry point for this area of law. *See A Conversation with Chief Justice John Roberts* (C-SPAN television broadcast June 25, 2011), https://www.c-span.org/video/?300203-1/conversation-chief-justice-roberts [https://perma.cc/XQ3X-EH5X] ("Pick up a copy of any law review that you see, and the first article is likely to be, you know, the influence of Immanuel Kant on evidentiary approaches in eighteenth-century Bulgaria, or something, which I'm sure was of great interest to the academic that wrote it, but isn't of much help to the bar."); *see also* IMMANUEL KANT, CRITIQUE OF PURE REASON 17–21 (F. Max Müller trans., 2d ed. Rev. 1922) (explaining that the mind structures experiences of reality, while the rules dictating reality are intrinsic to the mind and, accordingly, if these rules are identified then reality can be decoded).

8 *See* Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 193, 195, 201 (1890). Their analysis could not foresee the intrusiveness of technological devices that would pervade contemporary society. Had they done so, then perhaps they would have placed a premium on the intellectual activities ultimately at the center of what is to be protected, rather than the act of intrusion itself that society would not accept as reasonable.

9 *See id.*

by the Pew Research Center, ninety-three percent of adults said that being in control of who can get their information is important, while ninety percent said that controlling what information is collected about them is also important.[10] Nevertheless, billions of people willingly hand over their personal information every day without understanding the effects that this may have on their own privacy.[11]

This Article addresses the impact of the lack of oversight over the IoT, and the data-security and privacy issues that the IoT implicates. Part I provides a brief background of and defines the IoT, and discusses its interaction with data collection. Part II explains the current state of IoT privacy regulations under the federal framework, along with a discussion of California's lead on data privacy issues. Additionally, Part II briefly discusses a few successful attempts by the Federal Trade Commission ("FTC") to hold IoT developers accountable for security breaches. Part III discusses recent data-security issues and potential future harms to privacy in the IoT. In particular, this Part discusses recent IoT devices that have been hacked and the resulting injuries. Part IV discusses data-breach notifications, and the need for the FTC to—at minimum—include a privacy-by-design aspect in overseeing IoT devices. This Part also discusses self-help methods that consumers may apply to protect their data and privacy, and the potential impact that self-help might have on federal regulations.

I. A HISTORY OF THE INTERNET OF THINGS

The IoT is composed of mostly unsecure devices, which provide a wellspring of information about its users.[12] This Part

---

[10] Mary Madden & Lee Rainie, *Americans' Attitudes About Privacy, Security and Surveillance*, PEW RESEARCH CTR. (May 20, 2015), http://www.pewinternet.org/2015/05/20/americans-attitudes-about-privacy-security-and-surveillance/ [https://perma.cc/M75G-ADT9].

[11] *See, e.g.*, Ben Popper & Nikki Erlick, *Facebook Is Closing in on [Two] Billion Monthly Users*, VERGE (Feb. 1, 2017, 4:14 PM), http://www.theverge.com/2017/2/1/14474534/facebook-earnings-q4-fourth-quarter-2016 [https://perma.cc/E7TU-6FER].

[12] *See* Lucian Constantin, *IoT Malware Starts Showing Destructive Behavior*, PCWORLD (Apr. 7, 2017, 11:37 AM), http://www.pcworld.com/article/3188484/security/iot-malware-starts-showing-destructive-behavior.html [https://perma.cc/B4R7-8HUF].

provides a brief background of the IoT, defines some of its pertinent characteristics, and raises key issues on how the IoT relates to data collection and privacy.

A. A Brief Background on the IoT

Technologist Kevin Ashton claimed he coined the term "the Internet of Things" in 1999 during a presentation to Proctor and Gamble, in which he stated that adding radio-frequency identification ("RFID") and other sensors to everyday objects will lay the foundation of a new age of machine perception, creating an Internet of Things.[13] At the time, it seems that Ashton was primarily discussing the use of RFIDs in an industrial setting, since the idea of a networked manufacturing process dates back to the 1980s.[14] The development and ubiquity of RFIDs precipitated the growth of a larger growing body of interconnected devices for consumer use, where all devices are now becoming linked within a network.[15] Thus, "[w]hat makes the IoT dynamic is the ability to control products, machines and systems over the internet."[16]

It appears that the digital revolution has come full-circle. The IoT is not only a new realm unto itself; it also affects how the

---

[13] *See* Kevin Ashton, *That 'Internet of Things' Thing*, RFID J. (June 22, 2009), http://www.rfidjournal.com/articles/view?4986 [https://perma.cc/JFP6-83SV]; *see also* CLARITY INNOVATIONS, INTERNET OF THINGS 5 (2016), https://www.clarity-innovations.com/sites/default/files/publications/clarity-iot-in-education.pdf [https://perma.cc/9ETV-M5CF].

[14] *See A Sea of Sensors*, ECONOMIST (Nov. 4, 2010), http://www.economist.com/node/17388356 [https://perma.cc/6DPU-384T] ("The concept of the 'internet of things' dates back to the late 1980s, when researchers at Palo Alto Research Centre (PARC) in Silicon Valley imagined a future in which the virtual and the real world would be connected."); *see also, e.g.*, Lars S. Smith, *RFID and Other Embedded Technologies: Who Owns the Data?*, 22 SANTA CLARA COMPUTER & HIGH TECH. L.J. 695, 695–96 (2006) (discussing RFID's application to managing commercial inventory and manufacturing).

[15] *See, e.g.*, Alexandre Santos et al., *Internet of Things and Smart Objects for M-Health Monitoring and Control*, 16 PROCEDIA TECH. 1351, 1352 (2014) ("RFID[] is used in many applications . . . . There are several methods of identification, although the most common is a microchip able to store a serial number that identifies the person, object or thing. Using electronic devices that emit radio frequency signals, it is possible to perform an automatic capture of data, or a tag, from a reader.").

[16] H. Michael O'Brien, *The Impact of the Smart Home Revolution on Product Liability and Fire Cause Determinations*, WILSON ELSER (Sept. 12, 2016), https://www.wilsonelser.com/writable/files/Client_Alerts/product_liability_fire_science_.pdf [https://perma.cc/Y3DH-LR6L].

Internet works.[17] The Internet was once only comprised of codes in the abstract—ephemerally stored in the cloud.[18] However, the Internet has now manifested itself into the physical world in the form of networked objects also known as the IoT.[19] Courts and legislators are failing to address the appropriate level of oversight of developing technologies with privacy implications, such as IoT devices entering the market. Notably, this Article does not focus on one single device, and generally discusses the privacy issues that the IoT creates.

B. The IoT Defined

At its most basic definition, the IoT is simply objects with sensors networked together that are capable of communicating with one another.[20] The IoT is synonymous with smart cities, driverless cars, and all other forms of interconnected objects and wearables.[21] Born of innovation, these networked objects have

---

[17] Pierre DeBois, *How the Internet of Things is Reshaping Search*, CMS WIRE (Mar. 20, 2017), http://www.cmswire.com/digital-experience/how-the-internet-of-things-is-reshaping-search/ [https://perma.cc/2KJP-CNFZ] ("The quality of queries from IoTQR"—which is defined as the "search results based on the query phrases consumers say to a smart device"—"differs significantly from a search engine results page (SERP), making marketers reconsider how digital media should align to query phrases as well as with online search patterns of keywords.").

[18] *See* David Delony, *The [Five] Programming Languages that Built the Internet*, TECHOPEDIA (Oct. 3, 2014), https://www.techopedia.com/2/25666/internet/the-6-programming-languages-that-built-the-internet [https://perma.cc/5456-X55R] (explaining how the Internet was built on coding languages). *See generally* Steve Johnson, *What is Digital Coding?*, TECHWALLA, https://www.techwalla.com/articles/what-is-digital-coding [https://perma.cc/A9S2-YUVR] (last visited Aug. 24, 2017) (discussing the basics of digital coding and the binary system of zeros and ones that comprise the fundamental language of digital information).

[19] Luigi Atzori et al., *The Internet of Things: A Survey*, 54 COMPUTER NETWORKS 2787, 2787 (2010) ("The basic idea of this concept is the pervasive presence around us of a variety of things or objects—such as . . . RFID tags, sensors, actuators, mobile phones, etc.—which, through unique addressing schemes, are able to interact with each other and cooperate with their neighbors to reach common goals."); *see also* Jacob Morgan, *A Simple Explanation of the 'Internet of Things,'* FORBES (May 13, 2014), https://www.forbes.com/sites/jacobmorgan/2014/05/13/simple-explanation-internet-things-that-anyone-can-understand/#1910b3fb1d09 [https://perma.cc/3DK2-W3RA] (providing a visual aid to illustrate the interconnectivity of the IoT).

[20] *See* Atzori et al., *supra* note 19.

[21] *See* Jason Tanz, *The CIA Leak Exposes Tech's Vulnerable Future*, WIRED (Mar. 8, 2017, 12:00 PM), https://www.wired.com/2017/03/cia-leak-exposes-techs-vulnerable-

developed to improve the lives of their users.[22] Additionally, the technology provides for a real-time application of data processing, data storage, and data analysis.[23] These objects gather and collect data, for example, in order to remind you that it is time to take your pills.[24] On a larger scale, the so-called Industrial IoT is streamlining industrial production across the world.[25] However, what remains unclear is the depth and breadth of how these efficient objects will impact privacy.[26]

In order to anticipate the IoT's impact on daily life, a basic understanding of its mechanics is necessary. IoT devices share data using familiar network protocols such as Wi-Fi, Bluetooth, mobile phone networks, and specialized networks—as well as the global Internet.[27] IoT devices are embedded with RFIDs in order to share

---

future/ [https://perma.cc/XVV2-NMZX] ("Whether you call it the 'Internet of Things' or the 'Internet of Everything' or the 'Third Wave' or the 'Programmable World,' the long-predicted moment when connectivity becomes as ubiquitous as electricity is nearly upon us.").

22 Paul Kominers, *Interoperability Case Study: Internet of Things (IoT)*, BERKMAN CTR. FOR INTERNET & SOC'Y 3 (2012), https://cyber.law.harvard.edu/node/97248 [https://perma.cc/92EV-U5QE] ("The grand vision of the [IoT] is a world of networked intelligent objects. Every car, refrigerator, and carton of milk would be distinguished with its RFID chip, and they communicate constantly and seamlessly to create a much more efficient world.").

23 *See* Leon Hounshell, *Forecasting Profitable Models for the Internet of Things*, FORBES (Mar. 23, 2017), https://www.forbes.com/sites/forbestechcouncil/2017/03/23/forecasting-profitable-models-for-the-internet-of-things/#1f2d5cf33e94 [https://perma.cc/52AW-J32S].

24 *See* DAVID ROSE, ENCHANTED OBJECTS: DESIGN, HUMAN DESIRE, AND THE INTERNET OF THINGS 8–9 (2014) (discussing a pill bottle called a GlowCap that syncs to the Internet to remind patients to take their pills).

25 *See* Kipp Bradford, *The Industrial Internet of Things*, FORBES (Feb. 5, 2014, 8:00 AM), https://www.forbes.com/sites/oreillymedia/2014/02/05/the-industrial-internet-of-things/#7da766581c39 [https://perma.cc/DXM7-C9YX].

26 *See generally* RICHARD RUTLEDGE ET AL., GA. INST. OF TECH., DEFINING THE INTERNET OF DEVICES: PRIVACY AND SECURITY IMPLICATIONS (2014), https://smartech.gatech.edu/bitstream/handle/1853/52020/plsc2014-IoD.pdf [https://perma.cc/76TX-Y246].

27 *See* Ian Brown, GSR Discussion Paper: Regulation and the Internet of Things 3, 6 (June 25, 2015) (working paper) (on file with International Telecommunication Union), https://www.itu.int/en/ITU-D/Conferences/GSR/Documents/GSR2015/Discussion_papers_and_Presentations/GSR_DiscussionPaper_IoT.pdf [https://perma.cc/558E-MFMS] ("Machine-to-Machine (M2M) communication is used to refer to communication directly between IoT devices, often via cellular networks.").

data.[28] RFIDs are then connected to networked objects such as "parking meters, thermostats, cardiac monitors, tires, roads, car components, to supermarket shelves and many other types of physical object."[29] RFIDs are also being connected to what most would already consider a private object.[30] Driverless cars are quickly being developed with complex sensors that track and analyze a user's driving habits.[31] There are already plans to connect smartphones to parking grids in order to make parking efficient while maximizing public spaces.[32] In short, the IoT has arrived.

Unfortunately, many IoT devices are hastily put on the market and are not engineered to protect data security.[33] IoT developers are rushing their devices to market before properly ensuring that their devices are stable and secure.[34] Particularly, consumer-goods manufacturers—not computer software or hardware firms—often

---

[28] *See* HELEN NISSENBAUM, PRIVACY IN CONTEXT: TECHNOLOGY, POLICY, AND THE INTEGRITY OF SOCIAL LIFE 31–35 (2010) (discussing two types of RFIDS, active and passive—active RFIDs are internally powered, and can communicate over longer distances and up to one thousand meters while travelling at upwards of one hundred miles per hour, whereas a passive RFID is not internally powered and is only engaged when a reader is close in enough in proximity).

[29] Brown, *supra* note 27, at 3.

[30] *See* John Kennedy, *Intimate of Things: Smart Vibrator Gets Hacked at Def Con 24*, SILICON REPUBLIC (Aug. 10, 2016), https://www.siliconrepublic.com/machines/smart-vibrator-hacked-def-con-24 [https://perma.cc/5F36-3EQC]
(discussing a very private, if not very intimate, interconnected object named the "We-Vibe," a sex toy that is able to send information about its users, like the temperature of the device, each time a user changes intensity levels on the device).

[31] *See* Mike Ramsey, *On the Road to Driverless Cars*, FORBES (Jan. 26, 2017, 2:52 PM), https://www.forbes.com/sites/gartnergroup/2017/01/26/on-the-road-to-driverless-cars/#5d5c1b8617ed [https://perma.cc/QX76-VUFH].

[32] *See,* M. Ramya et al., *Parking Slot Availability Check and Booking System over IOT*, 1 ASIAN J. APPLIED SCI. & TECH. 149, 149–52 (2017) (discussing their design to improve and implement "Wi-Fi based smart car parking services in modern cities" to maximize public space and reduce waiting time).

[33] *See* Alisa Valudes Whyte, *Trending from CES: IoT Companies Avoiding Security Are Putting Their Survival at Stake*, HUFFPOST (Jan. 25, 2017, 8:53 AM), http://www.huffingtonpost.com/entry/trending-from-ces-iot-companies-avoiding-security_us_5888a8e2e4b04251e621fa88 [https://perma.cc/4ARX-DGY8].

[34] *See* Thibaut Rouffineau, *Three Flaws at the Heart of IoT Security*, UBUNTU INSIGHTS (Mar. 20, 2017), https://insights.ubuntu.com/2017/03/20/three-flaws-at-the-heart-of-iot-security/ [https://perma.cc/8GAY-ZEQT].

manufacture many IoT devices.[35] With little IoT developer oversight, and eroding federal regulations before they have even been established,[36] it is no wonder that the largest distributed denial of service attack ("DDoS") in history was perpetrated through a series of IoT devices.[37] A DDoS is a form of extortion by hackers, whereby a server is flooded with artificial traffic, bringing services to a screeching halt.[38] Accordingly, the IoT's rush to market and inherently flawed security poses several hazards to data-security and privacy.[39]

C. The IoT and Data Collection

In their seminal work on privacy, Samuel Warren and Justice Brandeis characterized an individual's privacy interest as the "right to be let alone,"[40] and defined this fundamental right in the context of "[r]ecent inventions" that threatened privacy.[41] "Recent inventions" such as the IoT, are potentially more pernicious and devastating to an individual's "right to be let alone,"[42] primarily because of the depth and breadth of information that IoT devices gather and analyze.

---

[35] Scott R. Peppet, *Regulating the Internet of Things: First Steps Toward Managing Discrimination, Privacy, Security, and Consent*, 93 TEX. L. REV. 85, 94 (2014).

[36] *See, e.g.*, S.J. Res. 34, 115th Cong. (2017) (disapproving 81 Fed. Reg. 87,274 (Dec. 2, 2016)).

[37] *See* Kim Zetter, *Hacker Lexicon: What Are DoS and DDoS Attacks?*, WIRED (Jan. 16, 2016, 7:00 AM), https://www.wired.com/2016/01/hacker-lexicon-what-are-dos-and-ddos-attacks/ [https://perma.cc/2JYU-W934] (discussing DDoS attacks); *see also, e.g.*, Lily Hay Newman, *What We Know About Friday's Massive East Coast Internet Outage*, WIRED (Oct. 21, 2016, 1:04 PM), https://www.wired.com/2016/10/internet-outage-ddos-dns-dyn/ [https://perma.cc/6LKM-X2GT]; *infra* Part III for an in-depth discussion of a recent DDoS attack through IoT devices.

[38] *See* Zetter, *supra* note 37.

[39] *See* Tom Pageler, *Is Everything Hackable in the Internet of Things?*, FORBES (Apr. 5, 2017, 8:00 AM), https://www.forbes.com/sites/forbestechcouncil/2017/04/05/is-everything-hackable-in-the-internet-of-things/#4bab849e3084 [https://perma.cc/WPS5-96HR] (discussing the lack of basic security controls for IoT devices).

[40] *See* Warren & Brandeis, *supra* note 8, at 193, 195.

[41] *Id.* at 195–96 (explaining that particularly threatening to privacy were the then new "business methods" whereby gossip had "become a trade").

[42] *See id.* at 205 ("The principle which protects personal writings and all other personal productions, not against theft and physical appropriation, but against publication in any form, is in reality not the principle of private property, but that of an inviolate personality.").

These IoT devices are engaging in "machine learning," by quickly identifying patterns as IoT users engage with the devices.[43] And even though consumers may not be aware, many of the devices already in use—and not necessarily associated with the IoT—are in fact capable of being tracked through unique identifiers embedded in devices such as cellphones.[44] By design, it appears that the IoT is bound to be a complex system of surveillance.[45] For example, "[i]f the information stored on an RFID-tagged consumer item is unique to the particular item, it can be used to distinguish the person carrying the item from all other persons and thus be used to track the person carrying the RFID-tagged item."[46]

Some scholars are skeptical of the blind-charge toward unfettered data collection.[47] Professor Neil M. Richards suggests, "Big Data is notable not just because of the amount of personal information that can be processed, but because of the ways data in one area can be linked to other areas and analyzed to produce new inferences and findings."[48] Nevertheless, scholars can agree that one problem is not necessarily the accuracy of the data collected,

---

[43] *See* PHILLIP N. HOWARD, PAX TECHNICA: HOW THE INTERNET OF THINGS MAY SET US FREE OR LOCK US UP 141 (2015) (defining machine learning as the process of how categories emerge from the data sets, rather than the old way of interpreting statistical data, which involved a hypothesis that was tested and crudely based on intuitive labels of factors thought to be effective to infer questions).

[44] *See* Gus Hosein & Caroline Wilson Palow, *Modern Safeguards for Modern Surveillance: An Analysis of Innovations in Communications Surveillance Techniques*, 74 OHIO ST. L.J. 1071, 1099 (2013); Paul M. Schwartz & Daniel J. Solove, *The PII Problem: Privacy and a New Concept of Personally Identifiable Information*, 86 N.Y.U. L. REV. 1814, 1837 (2011).

[45] *See* Nancy J. King, *When Mobile Phones Are RFID-Equipped—Finding E.U.-U.S. Solutions to Protect Consumer Privacy and Facilitate Mobile Commerce*, 15 MICH. TELECOMM. & TECH. L. REV. 107, 143–44 (2008) (discussing unique identifiers attributed to individual devices that create a system of surveillance).

[46] *Id.* at 143.

[47] *See, e.g.*, Paul Ohm, Response, *The Underwhelming Benefits of Big Data*, 161 U. PA. L. REV. 339, 345 (2013), http://www.pennlawreview.com/online/161-U-Pa-L-Rev-Online-339.pdf [https://perma.cc/4Q6V-7LCP] (urging caution in overestimating the benefits of Big Data, relative to the potential harms).

[48] Neil M. Richards, *The Dangers of Surveillance*, 126 HARV. L. REV. 1934, 1939 (2013) (providing a more in-depth discussion and analysis of Big Data, which is defined as large volumes of structured or unstructured data that organizations can potentially mine and analyze).

but the accuracy of the inferences drawn based upon the Big Data collected.[49] Professor Ryan Calo has even gone as far as to suggest that the aggregation and concentration of such private individual data could lead to what he calls "digital market manipulation."[50] "Digital market manipulation" could allow firms to "increasingly be able to trigger irrationality or vulnerability in consumers—leading to actual and perceived harms that challenge the limits of consumer protection law . . . which regulators can scarcely ignore."[51] Notwithstanding scholarly interpretation of the Big Data conundrum, immense data gathering and data storage is a source of collective anxiety.[52]

A major concern with Big Data regarding the IoT's privacy implications is that an individual's private information could be used to predict future behavior after it is aggregated and analyzed.[53] For example, "[s]ensor data capture incredibly rich nuance[s] about who we are, how we behave, what our tastes are, and even our intentions. Once filtered through 'Big Data' analytics, these data are the grist for drawing revealing and often unexpected inferences about our habits, predilections, and personalities."[54] Nevertheless, even with the growing concern over the IoT's impact on privacy, the Acting Chairman of the FTC, Maureen Ohlhausen, is pushing for IoT providers to self-regulate as part of the Trump administration's move toward complete deregulation.[55] In fact, the push toward deregulation has already

---

[49] *See* Omer Tene & Jules Polonetsky, *Big Data for All: Privacy and User Control in the Age of Analytics*, 11 NW. J. TECH. & INTELL. PROP. 239, 270–71 (2013) ("Inaccurate, manipulative, or discriminatory conclusions may be drawn from perfectly innocuous, accurate data.").

[50] Ryan Calo, *Digital Market Manipulation*, 82 GEO. WASH. L. REV. 995, 999 (2014).

[51] *Id.*

[52] *See* Quentin Hardy, *Rethinking Privacy in an Era of Big Data*, N.Y. TIMES (June 4, 2012, 9:55 AM), http:// bits.blogs.nytimes.com/2012/06/04/rethinking-privacy-in-an-era-of-big-data [https://perma.cc/AH3R-97V7] ("Privacy is a source of tremendous tension and anxiety in Big Data . . . . It's a general anxiety that you can't pinpoint, this odd moment of creepiness.").

[53] *See* Peppet, *supra* note 35, at 90.

[54] *Id.*

[55] *See* Sam Thielman, *Acting Federal Trade Commission Head: Internet of Things Should Self-Regulate*, GUARDIAN (Mar. 14, 2017, 6:00 AM), https://www.theguardian.com/technology/2017/mar/14/federal-trade-commission-internet-things-regulation [https://perma.cc/97LV-XFPN].

begun.[56] Based on the current state of the regulatory framework governing data-security and digital privacy, allowing manufacturers to self-regulate as the IoT develops could harm consumers and the IoT technology.[57] Accordingly, further deregulation, along with consumers failing to secure their information, could lead to a catastrophic breakdown in data security and privacy protections.

II. THE CURRENT STATE OF IOT REGULATIONS ON DATA-SECURITY AND PRIVACY

Our current privacy laws are collected in federal and state legislation; administrative agencies; and common-law actions in tort, property, and contract law.[58] This Part discusses federal and California regulations that govern digital privacy and security with respect to their impact on the IoT. Alarmingly, the trend toward deregulation is already taking hold.

Although consumers may have remedies in tort[59] or contract law,[60] these remedies may not provide proper relief.[61] For example, "[t]he current U.S. legal framework for cybersecurity is a

---

[56] *See infra* Part II.

[57] *See* Gareth Corfield, *[U.S.] Regulator Looks at Internet of Things Regulation, Looks Away*, REGISTER (Mar. 14, 2017), https://www.theregister.co.uk/2017/03/14/us_ftc_wont_start_internet_of_things_regulation/ [https://perma.cc/7S3L-DEEK].

[58] *See* PRISCILLA M. REGAN, LEGISLATING PRIVACY 70–88 (Univ. N.C. Press 1st ed. 1995).

[59] *See* Adam D. Thierer, *The Internet of Things and Wearable Technology: Addressing Privacy and Security Concerns Without Derailing Innovation*, 21 RICH. J.L. & TECH. 6, 102 (2015) (predicting that "[i]t would not be surprising to see future privacy-related controversies give rise to more legal actions involving the tort of intrusion upon seclusion"); Alexander H. Tran, Note, *The Internet of Things and Potential Remedies in Privacy Tort Law*, 50 COLUM. J.L. & SOC. PROBS. 263, 279–80 (2017) (arguing that public disclosure of private facts and intrusion upon seclusion might be adequate tort claims for IoT-related harms).

[60] *See* Stacy-Ann Elvey, *Hybrid Transactions and the Internet of Things: Goods, Services, or Software?*, 74 WASH. & LEE L. REV. 77, 158 (2017) (providing a thorough analysis of IoT's possible breach of warranty claims—for instance, some IoT devices sold to consumers contain hidden data monitoring features that are beyond the device's ordinary purpose, thus giving rise to a breach of warranty claim).

[61] *Cf.* Kevin L. Miller, *What We Talk About When We Talk About "Reasonable Cybersecurity": A Proactive and Adaptive Approach*, 90 FLA. B.J. 23, 23 (Sept.–Oct. 2016).

patchwork, consisting of a number of overlapping federal standards aimed at regulated entities in various sectors, state cyber-breach notification laws, state statutes, and caselaw arising from consumer's actions against companies."[62] Further, in federal courts, privacy claims in tort law must meet the requirements for Article III standing.[63] Additionally, if IoT related privacy issues were resolved under a tort theory like traditional privacy claims, the courts would be flooded with innumerable claims against IoT developers. And although a potential deluge of litigation might correct the current lackluster focus on security in the developing IoT market, it could take decades for such claims to travel through the state courts before developing into a cogent and predictable body of law.[64] Accordingly, the FTC and other agencies that regulate digital privacy are best suited to develop this emerging area of law, as discussed at length in the following section.

A. Federal Regulations of Data-Security and Privacy

In March 2017, a joint resolution in the House and Senate struck down Federal Communications Commission ("FCC") Chairman Tom Wheeler's regulation to protect Internet users'

---

62 *Id.*

63 The federal courts are of limited jurisdiction: claims must allege an injury-in-fact, causation, and redressability to satisfy the requirements of Article III standing, placing a heavy burden on the plaintiff, and thus creating another barrier to streamlining privacy-related issues related to the IoT. *See* Clapper v. Amnesty Int'l USA, 133 S. Ct. 1138, 1147–50 (2013) (holding that plaintiffs lacked standing because it was highly speculative that the government would in fact target plaintiff's communications, and thus there was no injury-in-fact); *see also* Obama v. Klayman, 800 F.3d 559, 561–62 (D.C. Cir. 2015) (per curiam) (holding that telecom subscribers did not have standing to challenge that the government's bulk data collection program—as authorized under the Patriot Act—violates the Fourth Amendment prohibition against unreasonable searches because plaintiffs could not demonstrate that they were, in fact, targeted for surveillance). *But see* Attias v. Carefirst, Inc., 865 F.3d 620, 629–30 (D.C. Cir. 2017) (holding that a class action had Article III standing, where the insured party suffered economic harm through having to purchase credit-monitoring services to prevent identity theft and fraud, which was not too speculative).

64 *Cf.* Andrew Meola, *The FAA Rules and Regulations You Need to Know to Keep Your Drone Use Legal*, BUS. INSIDER (July 25, 2017, 1:12 PM), http://www.businessinsider.com/drones-law-faa-regulations-2017-7 [https://perma.cc/T3CA-YFGR] (providing data indicating that drone regulation across the United States is nearing a decade long progression toward a cogent and predictable body of law).

personal information.[65] The now failed FCC regulation would have required Internet Service Providers ("ISPs")[66] to inform consumers what information was being collected and how that information was being used or shared.[67] The repeal's backers argued that the federal regulation would disadvantage ISPs in favor of other data-collecting companies like Google or Facebook—which the FTC oversees.[68] The FTC and the FCC are two distinct regulatory administrative agencies. Generally, the FTC oversees and approves large mergers,[69] regulates competition, and ensures consumer protection.[70] On the other hand, while the FCC regulates similar activity, the FCC does not focus on consumer protection.[71] The FCC is primarily engaged in "promoting competition, innovation and investment in broadband services and facilities."[72] Thus, the responsibility of online privacy regulation is likely to fall squarely on the FTC.[73]

---

[65] *See* S.J. Res. 34, 115th Cong. (2017) ("That Congress disapproves the rule submitted by the Federal Communications Commission relating to 'Protecting the Privacy of Customers of Broadband and Other Telecommunications Services' (81 Fed. Reg. 87,274 (Dec. 2, 2016) (to be codified at 47 C.F.R. pt. 64)), and such rule shall have no force or effect.").

[66] *Internet Service Provider (ISP)*, TECHOPEDIA, https://www.techopedia.com/definition/2510/internet-service-provider-isp [https://perma.cc/F84K-XZ8L] (last visited Oct. 14, 2017) ("An [ISP] is a company that provides customers with Internet access. Data may be transmitted using several technologies, including dial-up, DSL, cable modem, wireless or dedicated high-speed interconnects.").

[67] Protecting the Privacy of Customers of Broadband and Other Telecommunications Services, 81 Fed. Reg. at 87,275.

[68] Justin Cosgrove, *US Senate Votes to Repeal Internet Privacy Rules*, JURIST (Mar. 24, 2017, 10:32 AM), http://www.jurist.org/paperchase/2017/03/us-senate-votes-to-repeal-internet-privacy-rules.php [https://perma.cc/EW9E-NPVN].

[69] *See, e.g.*, Colin Lecher, *The FTC Says It Won't Stop Amazon from Buying Whole Foods*, VERGE (Aug. 23, 2017, 4:58 PM), https://www.theverge.com/2017/8/23/16193542/ftc-amazon-whole-foods [https://perma.cc/2LPG-KLQ6] (showing how the FTC approved Amazon's acquisition of Whole Foods).

[70] *About the FTC*, FED. TRADE COMM'N, https://www.ftc.gov/about-ftc [https://perma.cc/NX5S-ZDAQ] (last visited Oct. 25, 2017).

[71] *See What We Do*, FED. COMMC'NS. COMM'N, https://www.fcc.gov/about-fcc/what-we-do [https://perma.cc/49WG-KKBG] (last visited Oct. 25, 2017).

[72] *Id.*

[73] Caleb Chen, *Today, Senators Will Vote to Allow ISPs to Sell Your Internet History and End FCC Online Privacy Rules*, PRIVACY NEWS ONLINE (Mar. 23, 2017), https://www.privateinternetaccess.com/blog/2017/03/today-senators-will-vote-allow-isps-sell-internet-history-end-fcc-online-privacy-rules/ [https://perma.cc/DFU9-9S6Z] ("The resolution, if passed . . . would pass the responsibility of online privacy regulation from

Still, the Federal Trade Commission Act ("FTC Act") may be the best way to provide consumer relief.[74] Generally, the FTC has the authority to "gather and compile information concerning, and to investigate from time to time the organization, business, conduct, practices, and management of any person, partnership, or corporation engaged in or whose business affects commerce."[75] Primarily, the FTC oversees business that affects commerce through unfair practices.[76] The FTC Act is intended to prevent businesses "from using unfair methods of competition in or affecting commerce and unfair or deceptive acts or practices in or affecting commerce."[77] "Unfair" practices are defined as those that "cause[] or [are] likely to cause substantial injury to consumers which is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition."[78] Whereas a deceptive practice involves any misrepresentation of fact to any portion of the population.[79]

Though Federal legislation may regulate privacy matters in the IoT, the existing federal regulatory framework is scattered among several agencies.[80] For example, the Fair Crediting Report Act

---

the FCC onto the FTC . . . ."); Brian Fung, *The House Just Voted to Wipe Away the FCC's Landmark Internet Privacy Protections*, WASH. POST (Mar. 28, 2017), https://www.washingtonpost.com/news/the-switch/wp/2017/03/28/the-house-just-voted-to-wipe-out-the-fccs-landmark-internet-privacy-protections/?utm_term=.f5675f7787aa [https://perma.cc/ADS4-R42G] (stating that one critic discussing the bill remarked that "although consumers can easily abandon sites whose privacy practices they don't agree with, it is far more difficult to choose a different Internet provider").

74 *See* 15 U.S.C. § 45(a)(1) (2012) ("Unfair methods of competition in or affecting commerce, and unfair or deceptive acts or practices in or affecting commerce, are hereby declared unlawful.").

75 *Id.* § 46(a).

76 FED. TRADE COMM'N, *supra* note 70.

77 15 U.S.C. § 45(a)(2).

78 *Id.* § 45(n).

79 *See id.* § 45(a) ("Declaration of unlawfulness; power to prohibit unfair practices; inapplicability to foreign trade."). The FTC has defined an unfair practice as, inter alia, a deceptive practice or one that "creates a serious consumer injury," which must be substantial, and may include a practice that "does a small harm to a large number of people, or if it raises a significant risk of concrete harm." Int'l Harvester Co., 104 F.T.C. 949, 1064, 1073 n.12 (1984); *see also* Firestone Tire & Rubber Co. v. FTC, 481 F.2d 246, 251 (6th Cir. 1973).

80 *See generally* Fair Credit Reporting Act (FCRA), 15 U.S.C. §§ 1681–1681x (2012); Children's Online Privacy Protection Act of 1998 (COPPA), 15 U.S.C. §§ 6501–6506

("FCRA") applies to the collection of individual consumer information, and oversees the "[a]ccuracy and fairness of credit reporting."[81] The FTC Act authorizes the FTC to enforce any violations of the FCRA.[82] Although certain types of information like health and financial data are subject to heightened security requirements, there is no set statute that provides general data-security for back-office and other administrative operations involving personal information.[83] Accordingly, if an IoT provider violates the FCRA then a consumer might have a claim under that particular statute that is enforceable through the FTC Act.

For example, the FTC filed its first IoT related claim against TRENDnet in 2013, an IoT company that provided home webcam services, for failing to provide sufficient security measures to

---

(2012); Health Insurance Portability and Accountability Act of 1996 (HIPAA), Pub. L. No. 104-191, 110 Stat. 1936 (codified as amended in scattered sections of 18 U.S.C., 26 U.S.C., 29 U.S.C., 42 U.S.C.).

[81] *See* FCRA § 1681(a) ("Congress makes the following findings: (1) The banking system is dependent upon fair and accurate credit reporting. Inaccurate credit reports directly impair the efficiency of the banking system, and unfair credit reporting methods undermine the public confidence which is essential to the continued functioning of the banking system.").

[82] The FCRA provides that:

> It is the purpose of this subchapter to require that consumer reporting agencies adopt reasonable procedures for meeting the needs of commerce for consumer credit, personnel, insurance, and other information in a manner which is fair and equitable to the consumer, with regard to the confidentiality, accuracy, relevancy, and proper utilization of such information in accordance with the requirements of this subchapter.

§ 1681(b). Furthermore, according to the FTC:

> The Commission is hereby empowered and directed to prevent persons, partnerships, or corporations, except banks, savings and loan institutions described in section 57a(f)(3) of this title, Federal credit unions described in section 57a(f)(4) of this title, common carriers subject to the Acts to regulate commerce, air carriers and foreign air carriers subject to part A of subtitle VII of title 49, and persons, partnerships, or corporations . . . from using unfair methods of competition in or affecting commerce and unfair or deceptive acts or practices in or affecting commerce.

15 U.S.C. § 45(a)(2) (2012).

[83] *See* Paul M. Schwartz & Edward J. Janger, *Notification of Data Security Breaches*, 105 MICH. L. REV. 913, 922 (2006).

prevent hackers from intercepting access to its equipment.[84] TRENDnet provided "cameras for consumers to conduct security monitoring of their homes or businesses, by accessing live video and audio feeds ('live feeds') from their [Internet Protocol ('IP')] cameras over the Internet."[85] The FTC found that TRENDnet misrepresented its security measures, and failed to supply "reasonable security to prevent unauthorized access to sensitive information."[86] Hackers "compromised live feeds display[ing] private areas of users' homes and allowed the unauthorized surveillance of infants sleeping in their cribs, young children playing, and adults engaging in typical daily activities."[87] The FTC relied, in part, on the deception prong of the FTC Act because the FTC claimed that TRENDnet violated its own statements made to consumers.[88]

However, enforcement under the FTC Act for a company's general statements to consumers regarding security is typically difficult because it relies on a company "having made overly strong security-related promises to the public."[89] Since the security breach exposed sensitive information, the FTC determined that consumers' diminished ability to control the dissemination of their personal information resulted in significant harm.[90] The FTC recommended an updated and comprehensive security program, a new notice requirement, and a provision requiring TRENDnet to provide users with updated software to prevent the harm that the company had promised to secure consumers against.[91]

---

84 *See* Complaint at 1–4, TRENDnet, Inc., No. 122-3090, 2013 WL 4858250 (F.T.C. Sept. 3, 2013) [hereinafter TRENDnet Complaint].

85 *Id.* at 2.

86 *Id.* at 4. "[TRENDnet] described the IP cameras as 'secure' or suitable for maintaining security, including through . . . a sticker affixed to the cameras' packaging . . . which displays a lock icon and the word 'security.'" *Id.* at 3.

87 *Id.* at 5.

88 *Id.* at 6.

89 Peppet, *supra* note 35, at 136.

90 *See* TRENDnet Complaint, *supra* note 84, at 6.

91 *See* Press Release, Fed. Trade Comm'n, FTC Approves Final Order Settling Charges Against TRENDnet, Inc. (Feb. 7, 2014), https://www.ftc.gov/news-events/press-releases/2014/02/ftc-approves-final-order-settling-charges-against-trendnet-inc [https://perma.cc/9MSV-95NW] [hereinafter TRENDnet Press Release].

Most recently, the FTC filed a complaint against the Taiwan-based computer networking equipment manufacturer D-Link, alleging that the company failed to take reasonable steps to secure its wireless routers and IP cameras.[92] According to Jessica Rich, Director of the FTC's Bureau of Consumer Protection, "[h]ackers are increasingly targeting consumer routers and IP cameras—and the consequences for consumers can include device compromise and exposure of their sensitive personal information."[93] The complaint alleged that D-Link hard-coded login credentials into the camera software, thereby allowing access to consumers' live video and audio feeds; left users' login credentials unsecured on its mobile apps; and mishandled its own key code, allowing it to be public for six months.[94] Additionally, D'Link's "command injection flaws . . . allow[ed] remote attackers to gain control of consumers' devices,"[95] and was "a known vulnerability that lets attackers take control of people's routers and send them unauthorized commands."[96]

However, is FTC regulation over IoT providers trending toward deregulation or nonenforcement or deregulation through nonenforcement? Is this a distinction without a difference? Deregulation at this early stage of moving toward developing a cogent body of law that addresses IoT security issues would allow the market to dictate expectations rather than lawmakers and the courts. Earlier this year, the FTC voted two-to-one to authorize filing the complaint against D-Link; however, the acting FTC Commissioner, Maureen K. Ohlhausen, voted against the action.[97]

---

92 *See* Complaint at 5, FTC v. D-Link Corp., No. 3:17-cv-00039 (N.D. Cal. Jan. 5, 2017) [hereinafter D-Link Complaint].

93 Press Release, Fed. Trade Comm'n, FTC Charges D-Link Put Consumers' Privacy at Risk Due to the Inadequate Security of Its Computer Routers and Cameras (Jan. 5, 2017) (alteration to original), https://www.ftc.gov/news-events/press-releases/2017/01/ftc-charges-d-link-put-consumers-privacy-risk-due-inadequate [https://perma.cc/5BJQ-68GJ] [hereinafter D-Link Press Release].

94 D-Link Complaint, *supra* note 92, at 5.

95 *Id.*

96 Lesley Fair, *D-Link Case Alleges Inadequate Internet of Things Security Practices*, FED. TRADE COMM'N (Jan 5, 2017 1:04 PM), https://www.ftc.gov/news-events/blogs/business-blog/2017/01/d-link-case-alleges-inadequate-internet-things-security [https://perma.cc/UV9U-AKUE].

97 D-Link Press Release, *supra* note 93.

In 2014, the FTC voted unanimously to authorize filing the complaint against TRENDnet.[98] Recently, Commissioner Ohlhausen said that the FTC is "not primarily a regulator[,]" and the agency adopted a wait-and-see approach because there had been no real harm to consumers, despite the recent holdings in the *TRENDnet* and *D-Link* cases.[99] Although Congress has attempted to incentivize technology companies to adopt best practices,[100] the new trend in federal deregulation might just rewind the clock on the federal regulatory progress of IoT-related oversight.

The FTC has also brought claims against companies under the unfairness prong,[101] under which the FTC must demonstrate that a company's unfair practice caused or is likely to cause substantial harm to consumers.[102] With respect to financial and healthcare-related information, it is clear that the FTC has authority over such claims.[103] Unlike hidden telephone fees that accumulate and are traceable and predictable,[104] data security does not provide such a salient trail of bread crumbs. Although the FTC has prevailed in such actions,[105] the FTC's authority over data security requirements is limited, and would benefit from legislative action.

---

98 TRENDnet Press Release, *supra* note 91.

99 Thielman, *supra* note 55 (noting Ohlhausen also said "We're saying not 'Let's speculate about harm five years out,' but 'Is there something happening that harms consumers right now or is likely to cause harm to consumers'").

100 Data Breach Insurance Act, H.R. 6032, 114th Cong. § 45S (2016) (proposing to give a fifteen percent tax credit to companies that purchase data breach insurance coverage, and adopt the National Institute of Standard and Technology's voluntary cybersecurity framework).

101 *See* FTC v. Wyndham Worldwide Corp., 799 F.3d 236, 247 (3d Cir. 2015); LabMD, Inc. v. FTC, 776 F.3d 1275, 1277 (11th Cir. 2015); DSW Inc., 141 F.T.C. 117, 120 (2006); BJ's Wholesale Club, Inc., 140 F.T.C. 465, 468 (2005).

102 *See* 15 U.S.C. § 45(n) (2012).

103 *See generally* Andrew Serwin, *The Federal Trade Commission and Privacy: Defining Enforcement and Encouraging the Adoption of Best Practices*, 48 SAN DIEGO L. REV. 809, 829–30 (2011); Gerard M. Stegmaier & Wendell Bartnick, *Psychics, Russian Roulette, and Data Security: The FTC's Hidden Data-Security Requirements*, 20 GEO. MASON L. REV. 673, 688–89 (2013).

104 *See, e.g.*, FTC v. Inc21.com Corp., 745 F. Supp. 2d 975, 982 (N.D. Cal. 2010), *aff'd*, 475 F. App'x 106 (9th Cir. 2012).

105 *See, e.g.*, *Wyndham Worldwide*, 799 F.3d at 245–47 (holding that Wyndham's alleged failure to maintain reasonable and appropriate data security, if proven, could constitute an unfair method of competition in commerce).

Notably, several European countries are ahead of the regulatory curve of IoT oversight. In Germany and Norway, a seemingly innocuous blonde-hair blue-eyed doll named "Cayla" was banned.[106] Cayla is a smart and interactive fashion doll that many critics suggest is ripe for a security breach, revealing intimate details of its child-users, especially since the "voice recordings are stored and used for a variety of purposes beyond providing for the toys' functionality."[107] As the number of devices that data is gathered and stored in increases, so does the opportunity for a security breach.[108] In the United States, however, Cayla is free to enter the bedrooms of children whose parents are willing to fork over thirty-seven dollars.[109] The glaring difference between the United States and Germany is that German privacy laws are consolidated, while U.S. privacy laws are scattered among several agencies.[110] And as many of these agencies lose control in the oversight of IoT devices,[111] consumers will be left vulnerable to serious privacy invasions by devices with staggeringly weak encryption.[112] By consolidating federal regulations and establishing minimum standards, IoT developers would have clearer guidelines to adhere to before entering the market—similar to lawmakers in Germany.[113] Ultimately, federal regulatory

---

[106] Kimiko de Freytas-Tamura, *The Bright-Eyed Talking Doll That Just Might Be a Spy*, N.Y. TIMES (Feb. 17, 2017), https://www.nytimes.com/2017/02/17/technology/cayla-talking-doll-hackers.html?emc=edit_th_20170219&nl=todaysheadlines&nlid=58756048&_r=0 [https://perma.cc/7QBN-XYL2].

[107] *Id.*

[108] *See, e.g.*, *id.*

[109] Genesis, *My Friend Cayla Doll ([U.S.] Version), Incl. Mirror & Comb, 18" Tall*, AMAZON, https://www.amazon.com/Genesis-Toys-Friend-Interactive-Fashion/dp/B010T4JV5G [https://perma.cc/7XSA-C4TF] (last visited Oct. 16, 2017).

[110] *See* Daniel Dimov, *Differences Between the Privacy Laws in the EU and the US*, INFOSEC INST. (Jan. 10, 2013), http://resources.infosecinstitute.com/differences-privacy-laws-in-eu-and-us/#gref [https://perma.cc/VV4V-VU6C].

[111] *See, e.g.*, Cosgrove, *supra* note 68.

[112] *See* Lucian Constantin, *Popular Internet-of-Things Devices Aren't Secure*, COMPUTERWORLD (July 30, 2014, 4:22 PM), https://www.computerworld.com/article/2490587/networking/popular-internet-of-things-devices-aren-t-secure.html [https://perma.cc/TTR7-4RKW].

[113] *See* Tim Wybitul & Dr. Wolf-Tassilo Bohm, *German Parliament Passes New Federal Data Protection Act*, CHRON. DATA PROTECTION (May 2, 2017), http://www.hldataprotection.com/2017/05/articles/consumer-privacy/german-parliament-passes-new-federal-data-protection-act/ [https://perma.cc/GX29-W6ZZ] (discussing

oversight is the best way to address IoT data breaches that threaten privacy because it would provide clarity, settle expectations, and provide sufficient data security for consumers.

B. Expanding Data Breach Notifications

In light of these challenges, the existing federal data-breach notification laws should be expanded to include the IoT. According to Professor Scott R. Peppet, "a state could simply alter the definition of 'personal information' in their data-breach statute to include name plus biometric or other sensor-based data such as, but not necessarily limited to, information from fitness and health sensor devices; automobile sensors; home appliance, electricity, and other sensors; and smartphone sensors."[114] This approach would maintain the current practice "of applying data-breach notification statutes only to *already-identified* datasets . . . that include name[s] or other clearly identifying information."[115] This practical approach focuses on the type of information that an IoT device gathers, and would not interfere with the necessity of IoT developers' pragmatic market-reasons for collecting individual data, thereby maintaining individual privacy and market efficiency.[116]

The policy behind expanding data-breach notification laws to include IoT would serve the same purpose as it does for digital data. Disclosing IoT data breaches to the public serves a "reputational sanction" function, allowing consumers to mitigate harm from data breaches.[117] This expansion also affords a market mechanism to address data security, rather than an administrative

---

Germany's privacy laws under their forty-year old Federal Data Protection Act (*Bundesdatenschutzgesetz*—("BDSG")), which provides security minimums for developers to comply with, along with hefty fines for any violations).

114 Peppet, *supra* note 35, at 158.

115 *Id.*

116 *See* Adam Thierer, *Relax and Learn to Love Big Data*, U.S. NEWS (Sep. 16, 2013, 12:10 PM), https://www.usnews.com/opinion/blogs/economic-intelligence/2013/09/16/big-data-collection-has-many-benefits-for-internet-users (on file with Fordham Intellectual Property, Media & Entertainment Law Journal) (discussing the benefits of big data on consumers like "language translation tools, mobile traffic services, digital mapping technologies, spam and fraud detection tools, instant spell-checkers," and targeted consumer marketing).

117 Schwartz & Janger, *supra* note 83, at 918.

mechanism,[118] as this approach would provide a check on IoT device manufacturers.[119] Companies, developers, and corporate counsel have all shown that they take the reputational consequences of data-breach notification seriously because it affects their products.[120] For example, California has already issued general guidance on Internet data, as discussed in the following section.[121] Thus, legislators would need to specifically define personal information with respect to IoT devices' data-collecting capabilities. Nevertheless, the states should enact legislation to fill in the federal gaps.

C. After the Gold Rush: California on the IoT Data-Security and Privacy

The federal government's scattered sectoral approach to digital privacy issues has forced many states to address growing digital privacy issues, thus creating a patchwork of uncertainty.[122] In New York, legislators have adopted potent measures to ensure that financial companies protect consumer data.[123] However, California is one of forty-six states to enact data-breach notification laws,[124]

---

[118] *Compare* Mark Burdon, *Contextualizing the Tensions and Weaknesses of Information Privacy and Data Breach Notification Laws*, 27 SANTA CLARA COMPUTER & HIGH TECH. L.J. 63, 66 (2011) (noting that data-protection laws help mitigate market tensions between "consumer protection and corporate compliance cost minimization"), *with* Nathan Alexander Sales, *Regulating Cyber-Security*, 107 NW. U. L. REV. 1503, 1545 (2013) (identifying an administrative law approach to data security). *See generally* Calo, *supra* note 50 (discussing the concept of "market manipulation").

[119] *See* Burdon, *supra* note 118, at 66.

[120] *See* Kenneth A. Bamberger & Deirdre K. Mulligan, *Privacy on the Books and on the Ground*, 63 STAN. L. REV. 247, 275 (2010) ("[E]very single respondent mentioned . . . the enactment of state data breach notification statutes[] as an important driver of privacy in corporations." (citation omitted)).

[121] *See generally* OFFICE OF PRIVACY PROT., CAL. DEP'T OF CONSUMER AFFAIRS, RECOMMENDED PRACTICES ON NOTICE OF SECURITY BREACH INVOLVING PERSONAL INFORMATION 8–14 (2007).

[122] *See* Charlotte A. Tschider, *Experimenting with Privacy: Driving Efficiency Through a State-Informed Federal Data Breach Notification and Data Protection Law*, 18 TUL. J. TECH. & INTELL. PROP. 45, 52 (2015).

[123] *See* N.Y. COMP. CODES R. & REGS. tit. 23, § 500 (2017) (noting the need to establish regulatory minimum standards in order to resolve cybersecurity issues in the financial services industry).

[124] ALASKA STAT. § 45.48.010 (2008); ARIZ. REV. STAT. ANN. § 18-545 (West, Westlaw through 2017 1st Reg. Sess.); ARK. CODE ANN. § 4-110-105 (2017); CAL. CIV. CODE §§ 1798.29, 1798.82 (West 2016); COLO. REV. STAT. § 6-1-716 (West 2016); CONN. GEN.

not to mention a myriad of privacy regulations.[125] The California statute provides:

> Any agency that maintains computerized data that includes *personal information* that the agency does

---

STAT. § 36a-701b (West, Westlaw through 2017 Reg. Sess.); DEL. CODE ANN. tit. 6, § 12B-102 (2005), *amended by* Act of Aug. 17, 2017, ch. 129, sec. 1, § 12B-102, 81 Del. Laws (effective Apr. 14, 2018); FLA. STAT. ANN. § 817.568 (Westlaw through 2017 1st Reg. Sess. & 25th Leg., Spec. "A" Sess.); GA. CODE ANN. § 10-1-912 (2017); HAW. REV. STAT. §§ 487N-1–487N-7 (Westlaw through 2017 1st Spec. Sess.); IDAHO CODE. § 28-51-105 (2017); 815 ILL. COMP. STAT. 530/10–530/12 (West, Westlaw through P.A. 100-535); IND. CODE §§ 24-4.9-3-1–24-4.9-3-2 (2017); IOWA CODE ANN. § 715C.2 (2017); KAN. STAT. ANN. § 50-7a02 (2016); LA. STAT. ANN. § 51:3074 (2005) (effective Jan. 1, 2006), http://legis.la.gov/legis/Law.aspx?d=322030 [https://perma.cc/AEH4-K8LT]; ME. REV. STAT. tit. 10, § 1348 (2017); MD. CODE ANN., COM. LAW. §§ 14-3501–14-3508 (Westlaw through 2017 Reg. Sess.), *amended by* Personal Protection Act, ch. 518, sec. 1, §§ 14-501–508, 2017 Md. Laws 2755, 3080–89 (2017) (effective Jan. 1, 2018); MASS. GEN. LAWS ANN. ch. 93H, §§ 1–6 (West, Westlaw through 2017 1st Ann. Sess.); MICH. COMP. LAWS § 445.72 (2017); MINN. STAT. § 325E.61 (2006); MISS. CODE ANN. § 75-24-29 (2017); MO. REV. STAT. § 407.1500 (2009); MONT. CODE ANN. § 30-14-1704 (2017); NEB. REV. STAT. § 87-803 (2017); NEV. REV. STAT. ANN. § 603A.220 (West, Westlaw through 79th Legis. Sess.); N.H. REV. STAT. ANN. § 359-C:20 (West, Westlaw through 2017 Reg. Sess.); N.J. STAT. ANN. § 56:8-163 (West, Westlaw through L.2017); N.Y. GEN. BUS. LAW § 899-aa (McKinney, Westlaw through Leg. 2017, ch. 1–402); N.C. GEN. STAT ANN. § 75-65 (2017); N.D. CENT. CODE ANN. §§ 51-30-02–51-30-03 (Westlaw through 2017 Reg. Sess. of the 65th Legis. Assemb.); OHIO REV. CODE ANN. §§ 1347.12, 1349.19 (Westlaw through 2017 File 23 of the 132nd Gen. Assemb. (2017–2018) & 2017 State Issue 1); OKLA. STAT. tit. 74, § 3113.1 (2016); OR. REV. STAT. § 646A.604 (Westlaw through 2017 Reg. Sess.) (effective through Oct. 6, 2017); 73 PA. CONS. STAT. §§ 2301–2308, 2329 (2005); 11 R.I. GEN. LAWS § 11-49.3-4 (2015); S.C. CODE ANN. § 39-1-90 (2017); TENN. CODE ANN. § 47-18-2107 (2017); TEX. BUS. & COM. CODE ANN. § 521.053 (West 2015); UTAH CODE ANN. § 13-44-202 (West 2009); VT. STAT. ANN. tit. 9, § 2435 (2017), http://legislature.vermont.gov/statutes/section/09/062/02435 [https://perma.cc/845D-869N]; VA. CODE ANN. § 18.2–186.6 (2017); *id.* § 32.1–127.1:05 (2010); WASH. REV. CODE § 19.255.010 (2017); *id.* § 42.56.590 (2017); W. VA. CODE §§ 46A-2A-101–46A-2A-105 (West, Westlaw through 2017 2d Extraordinary); WIS. STAT. § 134.98 (2017); WYO. STAT. ANN. § 40-12-502 (2017).

[125] *See* Online Privacy Protection Act, CAL. BUS. & PROF. CODE §§ 22575–22579 (West 2017); Digital Privacy Rights for Minors, CAL. BUS. & PROF. CODE §§ 22580–22582 (Deering 2017); Student Online Personal Information Protection Act, CAL. BUS. & PROF. CODE §§ 22584–22585 (West 2017); Consumer Protection Against Computer Spyware Act, CAL. BUS. & PROF. CODE §§ 22947–22947.6 (West 2017); Medical Apps Act, CAL. CIV. CODE § 56.06 (West 2014), *amended by* Act of Oct. 7, 2017, ch. 561, sec. 17, § 56.06, 27, 2017 Cal. Leg. Serv. 1, 27–28 (West); Cyber Exploitation Act, CAL. CIV. CODE § 1708.85 (2014), *amended by* Act of Sept. 11, 2017, ch. 233, sec. 1, § 1708.85(f), 2017 Cal. Leg. Serv. 1, 2–4 (West) & CAL. PENAL CODE §§ 502.–502.01, 647(j), 647.8, 786 (West 2017); CAL. GOV. CODE § 11015.5 (West 2017).

> not own shall notify the owner or licensee of the information of any breach of the security of the data immediately following discovery, if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person.[126]

Personal information has either of two meanings. First, it means an individual's first name or first initial and last name, in combination with any of the following data elements: social security number, driver's license number, financial account number, medical information, or health insurance information.[127] Second, it means a username or e-mail address, in combination with a password or security question and answer that would permit online access of information.[128] However, personal information does not include "publicly available information that is lawfully made available to the general public from federal, state, or local government records."[129]

Defining and identifying data as personal or public is a start. For example, consider fitness and health related data: This likely qualifies as personal information, and is therefore protected under California statute, in part, because it is not publicly available.[130] As Professor Peppet suggested,[131] perhaps all of the data collected by IoT devices could be considered data that is related to health and fitness under the California statutory scheme.[132] For example, teakettles, pillboxes, and HVAC systems all implicate an individual's health-related habits, since they demonstrate the user's dietary habits, medical issues, and environmental surroundings.[133] Notwithstanding smart city devices and industrial devices,

---

126 CAL. CIV. CODE § 1798.29(b) (emphasis added).

127 *Id.* § 1798.81.5(d)(1)(A).

128 *Id.* § 1798.81.5(d)(1)(B).

129 *Id.* § 1798.81.5(d)(4).

130 *See* Peppet, *supra* note 35, at 139.

131 *See id.* at 158.

132 *See id.* With the exclusion of IoT devices such as bridge sensors, and other devices that do not monitor an individual's behavior.

133 *Cf.* Sam Thielman & Elle Hunt, *Cyber Attack: Hackers 'Weaponised' Everyday Devices with Malware*, GUARDIAN (Oct. 22, 2016, 1:47 AM), https://www.theguardian.com/technology/2016/oct/22/cyber-attack-hackers-weaponised-everyday-devices-with-malware-to-mount-assault [https://perma.cc/4QGY-PNR9] (discussing the sensitive information stored in everyday items such as teakettles).

personally identifiable IoT devices within the home likely provide insight into an individual user's health-related information.[134] Thus, defining IoT devices that encompass such broad health-related information—which is already protected under existing statutes—may provide legislators with the means to include more stringent protection for IoT data, and ultimately, the privacy of its users.

Furthermore, the California Online Privacy Protection Act ("CalOPPA") provides, in part, that website operators could be subject to legal action for failing to meet the standards outlined in the Act, which determine how a website operator must post their privacy policies.[135] CalOPPA was recently amended to require that privacy policies also identify the categories of personally identifiable information collected, and with what third parties that information will be shared.[136] Much like the FTC, CalOPPA is enforced by a separate Act known as the Business and Professions Code section 17200,[137] which provides the same causes of action as the FTC Act under either an unlawful or unfair prong.[138] California also provides similar guidance material on privacy notifications for emerging technology providers, although it is not enforceable.[139]

---

[134] *See, e.g.*, Marc Ambasna-Jones, *The Smart Home and a Data Underclass*, GUARDIAN (Aug. 3, 2016, 10:26 AM), https://www.theguardian.com/media-network/2015/aug/03/smart-home-data-underclass-internet-of-things [https://perma.cc/GU9X-EXSR] (discussing the benefits and perils of insurance companies gathering personal home data, and providing discounts or higher premiums depending on domestic habits).

[135] *See* CAL. BUS. & PROF. CODE §§ 22575–22579 (West 2017).

[136] *See* A.B. 370, 2013 (Cal. 2013).

[137] CAL. BUS. & PROF. CODE § 17200 (West 2017); *id.* §§ 22575–22579; CARTLON A. VARNER & THOMAS D. NEVINS, CALIFORNIA ANTITRUST AND UNFAIR COMPETITION 1–2 (3d ed. 2003) (noting that the California Supreme Court recognized section 17200 as the "little FTC Act").

[138] *See* BUS. & PROF. § 17200 ("[U]nfair competition shall mean and include any unlawful, unfair or fraudulent business act or practice and unfair, deceptive, untrue or misleading advertising . . . .").

[139] *See generally, e.g.*, KAMALA D. HARRIS, CAL. DEP'T OF JUSTICE, MAKING YOUR PRIVACY PRACTICES PUBLIC: RECOMMENDATIONS ON DEVELOPING A MEANINGFUL PRIVACY POLICY (2014), https://oag.ca.gov/sites/all/files/agweb/pdfs/cybersecurity/making_your_privacy_practices_public.pdf [https://perma.cc/73J9-GT5D] (including guidelines on how to "[m]ake it easy for a consumer to find the section in which you describe your policy regarding online tracking by labeling it").

Despite California's innovative strides toward regulating emerging technologies, it is still not prepared for the emerging privacy and security risks associated with the IoT. For example, IoT devices may not necessarily come shipped with privacy policies directly attached to the devices.[140] Additionally, IoT developers are rushing devices to the market, which are poorly equipped to provide adequate security.[141] Consumers will not be able to familiarize themselves with the device's privacy policies, or know if IoT providers are sharing their personal information and with whom, let alone enforce their purported privacy rights.

However, this may be changing. While CalOPPA may fail to keep pace with the IoT, California legislators are making strides to address the security issues that the IoT presents. Introduced by California Senator Hannah-Beth Jackson, Senate Bill 327 would require manufacturers selling connected devices to be equipped with "reasonable security features appropriate to the nature of the device and the information it may collect . . . that protect the device and any information contained therein from unauthorized access."[142] Further, the bill would require that manufacturers notify consumers of "*whether [a device] is capable of* collecting audio, video, *location, biometric, health, or other personal or sensitive user information if . . . not otherwise indicated by the*

---

[140] *See, e.g.*, Bernard Marr, *What Is the Internet of Things—A Complete Beginner's Guide in 2017*, FORBES (Apr. 10, 2017, 8:05 PM), https://www.forbes.com/sites/bernardmarr/2017/04/10/what-is-the-internet-of-things-a-complete-beginners-guide-in-2017/#5ca75fc25982 [https://perma.cc/KU7K-76BK] (characterizing the Amazon Echo as an IoT device); *Alexa Terms of Use*, AMAZON, https://www.amazon.com/gp/help/customer/display.html?nodeId=201809740 [https://perma.cc/36KU-DNR6] (last updated Oct. 24, 2017) (providing terms of use and privacy policy on Amazon's website and not on the actual device); *see also* Jonathon Hauenschild, *Lawmakers Must Clarify Privacy Protections for the Internet of Things*, HILL (Jan. 6, 2017, 7:00 AM), http://thehill.com/blogs/pundits-blog/technology/312968-lawmakers-must-clarify-privacy-protections-for-the-internet-of [https://perma.cc/33LL-QCDB].

[141] *See* Gareth Corfield, *Fix Crap Internet of Things Security, Booms Internet Daddy Cerf*, REGISTER (Mar. 21, 2017, 2:36 PM), https://www.theregister.co.uk/2017/03/21/vint_cerf_internet_things_security/ [https://perma.cc/DB38-MTGD] ("The biggest worry [Vint Cerf has] is that people building [IoT] devices will grab a piece of open source software or operating system and just jam it into the device and send it out into the wild without giving adequate thought and effort to securing the system and providing convenient user access to those devices.").

[142] S.B. 327, Reg. Sess. (Cal. 2017).

packaging . . . ."[143] It would also require manufacturers to "*obtain consumer consent before it collects or transmits information beyond what is necessary in order to fulfill a user transaction or for the stated functionality of the connected device . . . .*"[144]

In fact, California Senator Hannah-Beth Jackson used Cayla—the same cute little doll that drew the ire of German policy-makers—as an example of why this piece of legislation is so important.[145] While the bill provides precisely the types of security measures that would secure consumer data with respect to IoT devices, at the moment, the California Senate cannot seem to push it through.[146] Many privacy-interest and public-interest groups support the bill, including the Electronic Frontier Foundation,[147] while its opponents—including the California Chamber of Commerce—spent over ten million dollars lobbying against the bill.[148] Ultimately, it was short on votes and will likely face further revision—possibly even removing its most important safeguards.[149] Nevertheless, Part III discusses recent examples of why it might be necessary for California to push forward on Senate Bill 327 to move toward securing IoT devices, and provide a model for other states and perhaps even federal regulations.

III. SECURITY BREACHES AND INVASIONS OF PRIVACY IN THE IOT

It is happening again. The rise of IoT malware is reminiscent of the viruses, worms, and e-mail spam that crippled early Internet users, because most personal computers were not adequately secured, and companies that rushed to enter the market ignored or

---

143 *Id.*

144 *Id.*

145 *See* Dan Morain, *This Cute Doll Can Spy on Your Kid. Why Doesn't the Legislature Seem to Care?*, SACRAMENTO BEE (June 9, 2017, 6:00 AM), http://www.sacbee.com/opinion/opn-columns-blogs/dan-morain/article155217209.html [https://perma.cc/7MSF-72E9]; *see also supra* Section II.A.

146 *See* Morain, *supra* note 145.

147 *See id.*; *see also* S.B. 327, Reg. Sess.

148 *See* Morain, *supra* note 145.

149 *See id.*

did not understand the need for Internet security.[150] The same is true now for the IoT. This Part argues that IoT devices have, in fact, harmed consumers, and that merely permitting IoT developers to oversee and develop their own best practices will leave users vulnerable to dangerous IoT attacks and privacy breaches.

Several scholars have urged lawmakers to permit the IoT to develop with relatively little oversight.[151] However, the *TRENDnet* and *D-Link* cases notwithstanding, the IoT has profoundly impacted individual privacy in other areas besides live-stream interception.[152] For example, an Ohio man was arrested and convicted of arson after the police examined his heart monitor's recorded data.[153] A cardiologist reviewed the data that the police retrieved from the man's heart monitor, and concluded that he could not have been in the home during the fire, which was contrary to the Ohio man's initial statements to the police.[154] The cardiologist said that it was "'highly improbable' that a person with [his] medical condition could collect and remove the items in such a short period of time."[155] Although this data is retrievable under other legal theories in cases of criminal investigations, this case illustrates the highly intrusive nature of IoT devices and their effect on the legal landscape.

Furthermore, the IoT is vulnerable to security breaches.[156] Consider the Ohio man with the IoT heart monitor. Perhaps the data that IoT providers monitor, store, and stream is unsecure like the live-streams in *TRENDnet*. Such unfettered access to personal and private information is not only offensive, it is also potentially

---

150 Lily Hay Newman, *The Botnet That Broke the Internet Isn't Going Away*, WIRED (Dec. 9, 2016, 7:00 AM), https://www.wired.com/2016/12/botnet-broke-internet-isnt-going-away/ [https://perma.cc/3VZW-WFYG].

151 *See, e.g.*, Thierer, *supra* note 59, at 118 (discussing the negative impact that regulation would have on innovation).

152 Debra Cassens Weiss, *Data on Man's Pacemaker Led to His Arrest on Arson Charges*, ABA J. (Feb. 6, 2017, 7:00 AM), http://www.abajournal.com/news/article/data_on_mans_pacemaker_led_to_his_arrest_on_arson_charges/?utm_source=maestro&utm_medium=email&utm_campaign=weekly_email [https://perma.cc/73HL-C894].

153 *Id.*

154 *Id.*

155 *Id.*

156 *See generally* Julie Brill, *The Internet of Things: Building Trust and Maximizing Benefits Through Consumer Control*, 83 FORDHAM L. REV. 205, 210–12 (2014).

physically dangerous. Suppose a hacker was able to intercept the data streaming from the man's heart monitor and interpret it to track patterns associated with his heart rate. The hacker now has the ability to track the man's physical presence and state at any given moment—for example, the hacker could determine if the man was asleep or out for a jog—and potentially perpetrate a physical crime. Thus, as the IoT links the Internet back into the physical world, IoT hacks can and will have physical implications.

What seems clear is that a single vulnerable IoT device opens up a number of vulnerabilities in all other IoT devices connected through the same network.[157] In particular, most IoT devices are, and will continue to be, connected through home Wi-Fi networks, which are easy to breach.[158] So if one device connected to your home network is inadequately protected, a hacker could use that device to breach your entire network, and thereby compromise other IoT devices *and* non-IoT devices connected to the same network, like laptops and cellphones.[159] Furthermore, consumers connect their IoT devices through their home routers, which are notoriously unprotected[160] and pose a serious security risk.[161] Many existing devices and new IoT devices have minimal

---

[157] *See* Atzori et al., *supra* note 19, at 2787 ("The basic idea of this concept is the pervasive presence around us of a variety of things or objects—such as . . . [RFID] tags, sensors, actuators, mobile phones, etc.—which, through unique addressing schemes, are able to interact with each other and cooperate with their neighbors to reach common goals.").

[158] *See Verizon Launches National IoT Network*, YAHOO FIN. (Apr. 3, 2017), http://finance.yahoo.com/news/verizon-launches-national-iot-network-162100012.html [https://perma.cc/HYL9-JM4U] (noting that IoT devices will be linked predominantly by Wi-Fi).

[159] *See* Dan Goodin, *[Twelve] Million Home and Business Routers Vulnerable to Critical Hijacking Hack*, ARSTECHNICA (Dec. 18, 2014), https://arstechnica.com /information-technology/2014/12/12-million-home-and-business-routers-vulnerable-to-critical-hijacking-hack/ [https://perma.cc/24LU-MZH5]. *See generally* Pageler, *supra* note 39.

[160] *See* Dan Goodin, *supra* note 159; Brian Krebs, *Lizard Stresser Runs on Hacked Home Routers*, KREBS ON SECURITY (Jan. 15, 2015), http://krebsonsecurity.com /2015/01/lizard-stresser-runs-on-hacked-home-routers/ [https://perma.cc/8WEC-EVMQ].

[161] *See* Bruce Schneier, *Security Risks of Embedded Systems*, SCHNEIER ON SECURITY (Jan. 9, 2014, 6:33 AM), https://www.schneier.com/blog/archives/2014/01/security_risks_9.html [https://perma.cc/3SH8-YLGG] ("[H]undreds of millions of devices that have been sitting on the Internet, unpatched and insecure, for the last five to ten years . . . . We have an incipient disaster in front of us. It's just a matter of when.").

protection against security breaches.[162] Accordingly, IoT devices connected through home routers are low-hanging fruit for hackers.[163]

The recent large-scale DDoS attacks on IoT devices may be a harbinger of even more widespread attacks to come, at the frontlines of which are Bots.[164] Bots can steal data, send spam, and intercept devices, all of which gum-up a network to slow it down, while holding the server hostage and gaining sensitive user-data.[165] There are several types of Bots, but this Article focuses on a very recent and pugnacious manifestation employed to disable IoT devices: "Mirai."[166]

In September and October 2016, DDoS attacks on several IoT devices used the infamous Mirai botnet.[167] Daniel Miessler,

---

[162] *See* Cameron Abbott & Giles Whittaker, *Is Your IoT Device Putting You at Risk? Internet of Things*, NAT'L L. REV. (Mar. 21, 2017), http://www.natlawreview.com/article/your-iot-device-putting-you-risk-internet-things [https://perma.cc/R3CF-V5EV] ("A Tripwire study found [ninety-six percent] of surveyed IT pros expect to see an increase in security attacks on IoT.").

[163] *See* Newman, *supra* note 150 (explaining that attacks on IoT devices are "'accelerating because there's a wide-open, unprotected landscape that people can go to,' says Chris Carlson, [V]ice [P]resident of product management at Qualys. 'It's a gold rush to capture these devices for botnets.'"); *see also* John Leyden, *Sh . . . IoT Just Got Real: Mirai Botnet Attacks Targeting Multiple ISPs*, REGISTER (Dec. 2, 2016, 12:19 AM), https://www.theregister.co.uk/2016/12/02/broadband_mirai_takedown_analysis/ [https://perma.cc/SUC8-W78U].

[164] *See Bots, the Next Frontier*, ECONOMIST (Apr. 9, 2016), https://www.economist.com/news/business-and-finance/21696477-market-apps-maturing-now-one-text-based-services-or-chatbots-looks-poised [https://perma.cc/2Y4E-NQMB] (discussing the impending importance of bots and chatbots—a type of bot dedicated to learning and applying language in user applications).

[165] *See* Paul Sabanal, *Thingbots: The Future of Botnets in the Internet of Things*, SECURITY INTELLIGENCE (Feb. 20, 2016), https://securityintelligence.com/thingbots-the-future-of-botnets-in-the-internet-of-things/ [https://perma.cc/MJ7P-X853].

[166] *See generally* Tony Bradley, *How Amazon Echo Users Can Control Privacy*, FORBES (Jan. 5, 2017, 12:12PM), https://www.forbes.com/sites/tonybradley/2017/01/05/alexa-is-listening-but-amazon-values-privacy-and-gives-you-control/#59268c327ee6 [https://perma.cc/8B2R-AGAJ] ("'Privacy and security of IoT is big right now following recent attacks like the Mirai botnet and malware targeting specific brands of smart TVs,' declared Cris Thomas, a respected security expert and spokesperson for Tenable Network Security.").

[167] *See* Chris Williams, *Today the Web Was Broken by Countless Hacked Devices – Your [Sixty]-Second Summary*, REGISTER (Oct. 21, 2016, 9:45 PM), https://www.theregister.co.uk/2016/10/21/dyn_dns_ddos_explained/ [https://perma.cc/DRU8-XBKK] ("Mirai spreads across the web, growing its ranks of obeying zombies,

Director of Advisory Services at IOActive commented, "The current state of IoT security is in bad shape, and will get a whole lot worse before it gets any better. The Mirai botnet, which is powered by 100,000 IoT devices that are insecure by default, is just the most obvious and topical example."[168] The Mirai botnet is incredibly pernicious—it is difficult to contain since it lurks on IoT devices, and generally does not noticeably affect devices' performance.[169] Unlike early IoT-like devices, the IoT runs on traditional IPs, which are notoriously vulnerable to attack.[170] Even assuming the average IoT device user realized that something was wrong, users have "no direct way to interface with the infected product."[171] The average consumer does not know how to troubleshoot—let alone fix—any potentially compromised devices.

Several copycat DDoS attacks have sprung from the Mirai botnet attack.[172] The BrickerBot penetrates IoT devices and then spreads to non-IoT devices, thus infecting an entire network of devices and programs connected to the breached IoT device.[173] Additionally, the Amnesia botnet "exploits . . . remote code execution vulnerability by scanning for, locating, and attacking vulnerable systems."[174] What these DDoS attacks highlight is that the IoT devices entering the market must come with adequate security protocols.[175] Accordingly, federal regulation that imposes

---

by logging into devices using their default, factory-set passwords via Telnet and SSH. Because no one changes their passwords on their gizmos, Mirai can waltz in and take over routers, CCTV cameras, digital video recorders, and so on.").

168 Leyden, *supra* note 163.

169 Newman, *supra* note 150.

170 *See* Srini Avirneni, *The Rise of Open-Source Malware and IoT Security*, FORBES (Apr. 5, 2017, 7:00 AM), https://www.forbes.com/sites/forbestechcouncil/2017/04/05/the-rise-of-open-source-malware-and-iot-security/#5a20f72e4080 [https://perma.cc/DAF3-WNZG].

171 Newman, *supra* note 150.

172 *See* Constantin, *supra* note 12.

173 *See id.*

174 John Leyden, *'Amnesia' IoT Botnet Feasts on Year-Old Unpatched Vulnerability*, REGISTER (Apr. 7, 2017), https://www.theregister.co.uk/2017/04/07/amnesia_iot_botnet/ [https://perma.cc/Z4N9-HFTR].

175 *See* Avirneni, *supra* note 170.

stricter guidelines on IoT developers before entering the market would prevent future attacks.[176]

IV. SOLUTIONS FOR DATA-SECURITY AND PRIVACY IN THE IOT

If the FTC is trending toward deregulating the IoT and IoT purveyors are left to oversee themselves, then security and privacy will surely remain vulnerable. Perhaps the only sure-fire way to ensure the security of IoT devices and consumer privacy is to do it yourself. This Part argues that businesses would benefit from a self-imposed privacy-by-design scheme. Additionally, consumers should rely on self-help methods to ensure their privacy and security while also urging manufacturers to continue to utilize established best practices. However, self-help measures could negatively impact federal regulation of the IoT.

A. Privacy-by-Design in the IoT

The European Parliament and Council of Ministers has already been working to incentivize companies to incorporate security safeguards by-design[177] in order to protect user privacy.[178] Whereas the FTC:

> [S]uggests companies follow a 'defen[s]e in depth' approach, considering security measures at several different points in their systems, such as using access control measures and encrypting data even when users are making use of encrypted links to home Wi-Fi routers (which will not protect the data

---

[176] Even self-help would fall short of shoring up protections against sophisticated botnets like Mirai. *See infra* Section IV; *see also* Kyle York, *Dyn Statement on 10/21/2016 DDoS Attack*, ORACLE + DYN (Oct. 22, 2016), http://dyn.com/blog/dyn-statement-on-10212016-ddos-attack/ [https://perma.cc/7AC5-J9F6] (statement by Chief Strategy Officer of Dyn, Kyle York, discussing the tens of millions of discrete IP addresses associated with the Mirai botnet that were part of the attack).

[177] *See generally What Is Security by Design?*, LOGICWORKS (Jan. 5, 2017), http://www.logicworks.com/blog/2017/01/what-is-security-by-design/ [https://perma.cc/8754-GDB8] (defining security by design as a standardized and controlled approach to integrating security measurers into each product before it hits the market).

[178] *See generally Brown, supra* note 27.

> between the router and the company's servers, or if the router is badly configured).[179]

In the United States, several companies have rolled out services that have proven to be vulnerable to hacking and attacks.[180] By incorporating a by-design approach, companies would have to rigorously test their services and products in order to enter the market.[181] For example, when a new product enters the market, developers adhere to physical safety standards like seatbelts or blade guards. Similarly, a tech company would adhere to privacy safety standards when creating and designing a new device or application. Although this approach may cost companies time and money in developing a more secure service or product, it would prevent serious privacy intrusion, and would ultimately benefit the company by providing greater security against liability. Most importantly, it would provide consumers with a choice of which products and services to purchase with their privacy in mind.

The biggest boost in IoT security could come from simply providing a stronger data encryption for devices right out of the box. Data encryption is essentially a form of security that depends on what is being protected.[182] With respect to IoT, sensitive user

---

[179] *Id.*

[180] *See* Nick Bilton, *Keeping Your Car Safe From Electronic Thieves*, N.Y. TIMES (Apr. 15, 2015), https://www.nytimes.com/2015/04/16/style/keeping-your-car-safe-from-electronic-thieves.html [https://perma.cc/KP34-55UK] (observing that two teens with a device were able to unlock a Toyota Prius with a very affordable and available method called amplification); Andy Greenberg, *Hackers Remotely Kill a Jeep on the Highway—With Me in It*, WIRED (July 21, 2015, 6:00 AM), https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/ [https://perma.cc/M8W7-AW5P] (noting that after an experiment demonstrated how easy it would be to hack into Jeep's smart car, Chrysler issued a recall for 1.4 million vehicles already on the road).

[181] *See generally* ANN CAVOUKIAN, PRIVACY BY DESIGN: THE [SEVEN] FOUNDATIONAL PRINCIPLES: IMPLEMENTATION AND MAPPING OF FAIR INFORMATION PRACTICES (1995), https://iab.org/wp-content/IAB-uploads/2011/03/fred_carter.pdf [https://perma.cc/UPQ9-4AZH] (discussing the fundamental principles of privacy-by-design, which would require developers to create and design new technology with privacy in mind, and intentionally incorporate certain safeguards into new devices the same way that, for example, developers incorporate physical safety considerations).

[182] *See generally* JUSTIN BROOKMAN, THE CONNECTED WORLD: EXAMINING THE INTERNET OF THINGS (2015), https://cdt.org/files/2015/02/Brookman-Final-IoT-Testimony.pdf [https://perma.cc/J9JB-D66H] (discussing the notion that consumers might expect certain types of data to be collected—for example, a fitbit user might expect to have data collected on his or her physical activity, but not any other data outside of the

data needs to be protected. Similar to the existing data-encryption[183] shielding personal information from the public, the IoT must rely on—at a minimum—what consumers have come to expect from their non-IoT devices—such as cellphones and laptops—to provide a basic level of security through encryption. However, many of the IoT devices that enter the market are not equipped with what consumers have come to expect as a basic level of cyber security.[184]

IoT developers should only be permitted to enter the market after proving up adequate security measures because default device encryption leaves IoT devices exposed to security breaches.[185] Although the costs of creating and maintaining adequate security will likely increase the prices of IoT devices entering the market,[186] the gains in security should be touted as a marketable benefit to the consumer—a benefit that, in light of recent DDoS attacks, should be just as important as the underlying service that a particular IoT device provides. Accordingly, both IoT developers and IoT users would benefit from clear design standards to ensure an IoT device's security. But if the market lags in dictating the security measures that IoT developers take before entering the market, perhaps consumers should take their data security and privacy concerns into their own hands.

---

expected use of a particular device); Nate Lord, *What is Data Encryption?*, DIGITAL GUARDIAN (July 27, 2017), https://digitalguardian.com/blog/what-data-encryption [https://perma.cc/6BMV-G4MH].

[183] *See* Lord, *supra* note 182 (defining data encryption as the process of transforming one piece of information into another form in order to hide its contents).

[184] *See* Noah Gamer, *Internet of Things—or Internet of Cyber Crime?*, TREND MICRO (Feb. 29, 2016), http://blog.trendmicro.com/internet-of-things-or-internet-of-cyber-crime/ [https://perma.cc/6KNR-2A4N].

[185] For example, if someone knows the default or factory password of a device, then they have access to "any device once it leaves the factory and is connected to the Internet." PHILLIP N. HOWARD, PAX TECHNICA: HOW THE INTERNET OF THINGS MAY SET US FREE OR LOCK US UP 3 (2015).

[186] *See* Pageler, *supra* note 39 ("It is important to realize that when building a device, the profit margins are slim, which leads to manufacturers avoiding adding anything to the bill of materials (BOM) cost. Anything added to the BOM, such as security hardware chips, gets passed onto the consumer five-fold.").

B. Self-Help: Blockchain Technology

There is a promising data security technology on the horizon. Blockchain technology ("BT") is a relatively new method of data encryption that has only been applied in financial technology.[187] Canadian programmer Vitalik Buterin describes BT as "decentrali[z]ed autonomous organi[z]ations" that are sets of rules for users to abide by,[188] and envisions BT allowing IoT devices to bypass registration and tracking.[189] BT is considered by many technology professionals and analysts to be the missing link to ensure data privacy.[190] BT essentially provides IoT providers with a lock and key to data.[191] BT can be used to track billions of IoT devices, and process and coordinate between devices by decentralizing the data.[192] Decentralization, along with stronger encryption, would provide stronger data security, thereby providing IoT users with more privacy.[193] There are companies cropping up all over the world that are developing BT's application

---

[187] *See* Bernard Marr, *How Blockchain Technology Could Change the World*, FORBES (May 27, 2016, 2:46 AM), https://www.forbes.com/sites/bernardmarr/2016/05/27/how-blockchain-technology-could-change-the-world/#3a76d254725b [https://perma.cc/L5LG-UAPG].

[188] *The Great Chain of Being Sure About Things*, ECONOMIST (Oct. 31, 2015), http://www.economist.com/news/briefing/21677228-technology-behind-bitcoin-lets-people-who-do-not-know-or-trust-each-other-build-dependable [https://perma.cc/FK36-R9MV].

[189] *See id.* ("Further out, some talk of using the technology to make by-then-self-driving cars self-owning, to boot. Such vehicles could stash away some of the digital money they make from renting out their keys to pay for fuel, repairs and parking spaces, all according to preprogrammed rules.").

[190] *See, e.g.*, Mark van Rijmenam, *What Is the Blockchain and Why Is It So Important?*, DATAFLOQ (Aug. 31, 2016), https://datafloq.com/read/what-is-the-blockchain-and-why-is-it-so-important/2270?utm=internal [https://perma.cc/468L-H4F5].

[191] Rohini Samtani, *Embracing the Internet of Things Doesn't Necessarily Mean Forfeiting Privacy*, CNBC (Mar. 28, 2017), http://www.cnbc.com/2017/03/29/embracing-the-internet-of-things-doesnt-necessarily-mean-forfeiting-privacy.html [https://perma.cc/Q7NB-Q82P].

[192] van Rijmenam, *supra* note 190 ("The data records, which can be a Bitcoin transaction or a smart contract or anything else for that matter, are combined in so-called blocks. In order to add these blocks to the distributed ledger, the data needs to be validated by [fifty-one percent] of all the computers within the network that have access to the Blockchain.").

[193] *See id.*

to IoT devices.[194] Most famously, BT was part of the driving technology that made Bitcoin so secure.[195] IBM, Microsoft, and many other service providers are also developing BT.[196] In a recent report, IBM suggested that attempting to monitor billions of IoT devices centrally would make them vulnerable to hacking and government surveillance.[197]

BT would also help to protect IoT devices from hackers and DDoS attacks. Business and technology expert Ahmed Banafa argues that there is an "urgent need for a secure IoT model to perform common tasks such as sensing, processing, storage, and communicating."[198] He argues that BT's edge is that it is public, and that everyone participating can see the blocks and any transactions stored inside of the block.[199] Although public, only those users with a private key may access their own blocks.[200] Since BT decentralizes all of the data, "there is no single authority that can approve transactions or set specific rules to have transactions accepted."[201] Although this decentralized data concept

---

[194] Companies are already providing BT services for IoT developers that want their devices to enter the market secure and stable. *See, e.g.*, BLOCKCHAIN OF THINGS, INC., CATENIS ENTERPRISE™ BY BLOCKCHAIN OF THINGS: A SECURE OPEN COMMUNICATION PLATFORM FOR IIOT INTEGRATION 1–2 (2017), https://daks2k3a4ib2z.cloudfront.net/59d018eaa992ae00015f3c40/5a00de1bd4ae9c0001c11200_CatenisDataSheet.pdf [https://perma.cc/JAN9-A7CF] ("Catenis Enterprise™ supports cross-platform integration and the rapid enablement of secure messages, immutable storage, smart properties, smart contracts, and digital asset transmissions.").

[195] *See* ECONOMIST, *supra* note 188.

[196] *See* Karla Lant, *Visa, Microsoft, and IBM Are All Hiring Blockchain Developers*, FUTURISM (Aug. 9, 2017), https://futurism.com/visa-microsoft-and-ibm-are-all-hiring-blockchain-developers/ [https://perma.cc/78XD-P38J].

[197] *See* IBM INST. FOR BUS. VALUE, DEVICE DEMOCRACY: SAVING THE FUTURE OF THE INTERNET OF THINGS 1 (2015), https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?subtype=XB&infotype=PM&appname=GBSE_GB_TI_USEN&htmlfid=GBE03620USEN&attachment=GBE03620USEN.PDF [https://perma.cc/YCK8-GBQA].

[198] Ahmed Banafa, *A Secure Model of IoT with Blockchain,* OPENMIND (Jan. 5, 2017), https://www.bbvaopenmind.com/en/a-secure-model-of-iot-with-blockchain/?utm_source=views&utm_medium=article06&utm_campaign=MITcompany&utm_content=banafa-jan07 [https://perma.cc/7VTM-HD4V].

[199] *See id.*

[200] *See* Samtani, *supra* note 191.

[201] Banafa, *supra* note 198.

is based on trust among its users, it is touted as the most secure response to privacy concerns for IoT devices.[202]

To be sure, BT is not without its flaws. Developers have raised concerns with scalability issues, processing power and time, storage, and legal and compliance issues that might scare off new businesses from integrating BT into their IoT devices.[203] At present, such diverse types of IoT devices would make it difficult to streamline BT.[204] Since BT is decentralized, the blocks would have to be housed in each individual IoT device; however, the sensors for most IoT devices are too small and do not have enough processing power.[205] Additionally, many—if not most—consumers may not have financial or informational access to such technology to ensure their data privacy. Nevertheless, BT provides the most promising prospect of securing data and promoting privacy in the IoT.

C. Self-Help Could Negatively Impact Potential Regulation

Consumer-wide self-help might run the risk of negatively impacting the policy that shapes eventual IoT regulation.[206] Although imperfect, BT could privatize and decentralize data-security.[207] Self-help measures like BT might run the risk of loosening the expectations of IoT developers to provide safe and secure IoT devices. Effectively, BT could provide enough security that legislators may not need to regulate the IoT. Self-help should remain a solution for consumers to combat the risks of data-security affecting privacy in an unregulated IoT world, without shifting entirely the burden from IoT developers to the consumer. But the complexity of the data-security and privacy issues from the IoT may prove unpredictable for self-help measures like BT.

---

202 *See* van Rijmenam, *supra* note 190.

203 *See, e.g.*, Alan R. Earls, *Blockchain for IoT Extends Beyond Ensuring Security*, IOT AGENDA (Apr. 2017), http://internetofthingsagenda.techtarget.com/feature/Blockchain-for-IoT-extends-beyond-ensuring-security [https://perma.cc/VP3B-TWTA].

204 *See* Banafa, *supra* note 198.

205 *Id.*

206 *See* Anita L. Allen, *An Ethical Duty to Protect One's Own Information Privacy?*, 64 ALA. L. REV. 845, 850 (2013).

207 *See* Banafa, *supra* note 198.

Furthermore, BT is user-based and still susceptible to hacks. Less than a year ago, Bitcoin was hacked for sixty-five million dollars.[208] While BT could provide strong encryption methods for IoT users, a modicum of oversight would still be necessary to address the data-security and privacy issues raised by IoT devices. In order to secure IoT devices and promote digital privacy, FTC regulations should include strict IoT developer oversight, and a more expanded definition of personal information, to promote effective data-breach notifications. This would not only promote digital privacy, but it would also provide a minimum expectation of individual privacy protection to IoT consumers. Accordingly, even with effective self-help methods like BT soon to be available to consumers, it may all be for naught unless regulators step in to provide meaningful guidance.

CONCLUSION

While the benefits of the developing IoT and its related technology provide a boon for users and the economy, it also provides pitfalls and potential legal challenges. As this technology develops and impacts daily life, it will be imperative to consciously and carefully develop the law alongside it. First, IoT developers should employ a privacy-by-design approach to their IoT devices before entering the market, which would benefit both developers and consumers. Second, perhaps California—among other states—might lead the way to a workable regulatory framework to ensure consumer data-security and privacy. With enough success, perhaps federal regulations will follow states like California, and streamline expectations for IoT developers and users. Finally, despite the potential impact to federal regulations of the IoT, consumers should protect their own data and privacy interests through available self-help measures, like BT. Thus, even though federal and state regulatory oversight would be ideal, until

---

[208] Yuji Nakamura & Lulu Yilun Chen, *Bitcoin Plunges, Rebounds After Hackers Steal [Sixty-Five] Million [Dollars]*, BLOOMBERG: TECH. (Aug. 2, 2016), https://www.bloomberg.com/news/articles/2016-08-03/bitcoin-plunges-after-hackers-breach-h-k-exchange-steal-coins [https://perma.cc/J9ME-T7X7].

then, consumers and service providers could utilize self-help methods like BT.