Washington University Jurisprudence Review

Volume 11 | Issue 2

2019

Privacy and the Internet of Things: Why Changing Expectations Demand Heightened Standards

Graham Johnson

PRIVACY AND THE INTERNET OF THINGS: WHY CHANGING EXPECTATIONS DEMAND HEIGHTENED STANDARDS

GRAHAM JOHNSON*

ABSTRACT

Entertainment consoles, wearable monitors, and security systems. For better or worse, internet-connected devices are revolutionizing the consumer products industry. Referred to broadly as the Internet of Things (IoT), this 'smart' technology is drastically increasing the means, scope, and frequency by which individuals communicate their personal information. This Note explores the disruptive impact of IoT consumer devices on the U.S.'s patchwork system of privacy protections. After presenting a high-level survey of several key regulatory issues, this Note argues that the proliferation of IoT devices exposes a fundamental flaw in the Katz "reasonable expectation of privacy" standard. As individual expectations of privacy rapidly and inevitably deteriorate, societal norms will follow suit, resulting in a Fourth Amendment standard, which is incompatible and outdated in this new, interconnected reality.

INTRODUCTION

On the morning of November 22, 2015, Victor Collins was found dead, floating in a patio hot tub behind James Bates' house in Bentonville, Arkansas.[1] Bates said the two friends were hanging out and drinking the previous evening, and he believed that Collins had accidentally drowned in the hot tub sometime after Bates had gone to bed around 1:00AM. Police quickly suspected foul play. Investigators noticed curious water marks on the patio, suggesting Bates may have sprayed it down to clean up blood or other evidence. They also noted potential signs of a struggle in the living room.[2] Despite the suspicious circumstances, however, the evidence was inconclusive.

---

* J.D. Candidate, Washington University School of Law Class of 2019.

1. Zuzanna Sitek & Dillon Thomas, *Bentonville PD Says Man Strangled, Drowned Former Georgia Officer*, 5 NEWS ONLINE (Feb. 23, 2016), http://5newsonline.com/2016/02/23/bentonville-pd-says-man-strangled-drowned-former-georgia-officer/.

2. *Id.*

What initially began as a typical murder investigation soon made national headlines. Investigators noticed that Bates had an Amazon Echo™ (a popular voice-activated speaker) set up in the living room where the struggle allegedly occurred. Believing the Echo might have inadvertently picked up and recorded some relevant evidence, investigators filed an administrative subpoena on Amazon, requesting the Echo's records from that evening.[3] Amazon pushed back against the request, asserting: "Given the important First Amendment and privacy implications at stake, the warrant should be quashed unless the Court finds that the State has met its heightened burden for compelled production of such materials."[4] Amazon's defiant response reignited a heated national conversation about the competing interests between consumer privacy and law enforcement—a debate initially sparked by Apple's high-profile refusal to unlock the San Bernardino shooter's iPhone just one year earlier.[5]

This time, however, the debate quickly subsided. Whatever data the Echo™ might have picked up became moot, as a different "smart" Internet-connected device provided investigators with the information they believed they needed to disprove Bates' story. Each new home in Bentonville came pre-installed with an Internet-connected utility meter. The meter "measure[d] and record[ed] the exact consumption of electricity and water per hour,"[6] which it then transmitted to the local utility company for processing and storage.[7] Hoping to shed some light on the patio water marks, investigators filed an administrative subpoena on the utility company. Unlike Amazon, the utility company did not challenge the request. The data revealed that on the night of Collins' death, 140 gallons of water were used at Bates' home between 1:00 – 3:00AM, while only 10 gallons were used while the men were awake together earlier in the evening. Investigators interpreted the excessive water usage to indicate foul play, suggesting the usage "was consistent with spraying down the back patio area."[8] Bates was subsequently charged with first-degree murder and tampering, at least in part on the basis of the utility meter evidence.[9]

---

3. Kim Lacapria, *Amazon Fights Subpoena for Alexa Data in Murder Investigation*, SNOPES (Feb. 23, 2017), https://www.snopes.com/news/2017/02/23/amazon-subpoena-alexa-data-murder/.

4. *Id.*

5. Amy B. Wang, *Police Land Amazon Echo Data in Quest to Solve Murder*, CHI. TRIB. (Mar. 9, 2017, 11:08 AM), http://www.chicagotribune.com/bluesky/technology/ct-amazon-echo-murder-wp-bsi-20170309-story.html.

6. *Id*.

7. *Id.*

8. *Id.*

9. However, the charges against Bates were eventually dismissed by the prosecution. In an interesting turn of events, Bates recently filed a lawsuit against the city of Bentonville and several

Casual Echo™ owners and privacy advocates alike were relieved that Amazon pushed back against the Bentonville investigators' request, but the fact that investigators believed they solved the case merely by analyzing data from an innocuous and unavoidable Internet-connected utility meter raises fresh questions of its own. How much data do Internet-connected devices collect about us in our daily lives? What does that data look like and reveal about us? How exactly is personal data collected, stored, and protected, both from malicious hackers and governmental interests? Perhaps most significantly, do we have any say over whether this data is collected in the first place?

These questions lie at the heart of the rapid technological development and societal implementation of intra- and Internet-connected devices, referred to broadly as the "Internet of Things" (IoT). There is no single, comprehensive definition for the Internet of Things. The Federal Trade Commission defines it as an "interconnected environment where all manner of objects have a digital presence and the ability to communicate with other objects and people."[10] The analytics firm McKinsey Global Institute defines the IoT: "[S]ensors and actuators connected by networks to computing systems."[11] The term is used both as a noun (e.g. the Internet of Things as an interconnected environment of devices) as well as an adjective (e.g. an IoT device). In this note, the IoT is most often used in the latter format as a descriptive term for consumer products (known colloquially as "smart" devices) that collect user data via built-in sensors and convey that data, both to each other and/or to centralized locations, through the Internet.

Part I will analyze the prevalence of consumer-oriented IoT devices in our society, discussing the diverse classes of data collected by IoT devices, the extensive scope of IoT data collection, and the various systems facilitating data collection. Part II will summarize four pressing real-world issues at the forefront of the IoT debate: 1) Unavoidable and comprehensive IoT data collection; 2) Lack of notice to consumers and general public ignorance of the extent of IoT data collection; 3) Inadequate data security facilitating targeted hacking and threatening the evidentiary

---

individuals involved in the murder investigation. Bates alleges that Bentonville police officers falsified reports and fabricated the results of an autopsy to make it appear as though Collins' death was a homicide. He maintains Collins' death was an accidental drowning. Tracy Neal, *Suit Accuses Police in Arkansas of Plot to Frame Man for Murder*, NW. ARK. DEMOCRAT GAZETTE (Jan. 28, 2019), https://www.nwaonline.com/news/2019/jan/28/suit-accuses-bentonville-police-of-plot/.

10. Jamie Lee Williams, *Privacy in the Age of the Internet of Things*, 41 HUM. RTS. 14, 16 (2015).

11. James Manyika et al., *The Internet of Things: Mapping the Value Beyond the Hype*, MCKINSEY GLOBAL INST. 1, n.1 (2015).

validity of IoT data; and 4) Unfair and unethical evidentiary inferences enabled by the admission of IoT data. Part III will outline the current legal landscape surrounding the IoT and the current trends and standards with regard to the admissibility of IoT data. Part III will also touch on the FTC's regulatory powers in the IoT sphere, the self-policing trends within the IoT product industries, and the limited regulatory roles of state and federal legislatures.

Part IV will then explore why the prevailing Fourth Amendment legal standard underlying privacy rights, namely an individual's protection against warrantless searches and seizures where that individual has a "reasonable expectation of privacy,"[12] is a fundamentally flawed approach to protecting privacy interests in light of the complex issues presented by IoT data collection. This Note will argue that the reasonable expectation standard is theoretically outdated due to shifting social norms, as well as practically ineffectual given the nature and degree of data collection by IoT devices. Instead of continuing to rely on an outdated legal standard, this Note advocates for a shift in the way the courts assess privacy interests in the IoT sphere. Rather than focus on subjective expectations of privacy, courts should instead consider an individual's right to privacy as a function of his or her right to control when, how, and to what extent their personal information is communicated to others.[13]

I. OVERVIEW OF THE INTERNET OF THINGS

While the phrase "Internet of Things" may be foreign to some, it is far from an unfamiliar concept in our increasingly interconnected society. Simply put, any device that 1) has a unique Internet Protocol (IP) address and 2) can connect to the Internet and transfer data with any degree of complexity is classified as an IoT device.[14] IoT devices, which can be both wired and wireless, utilize sensors to gather various forms of data, send the data across the Internet, and use the data to execute specific functions.[15] Cell phones, wearable devices (e.g. FitBits™ and Apple Watches™), entertainment consoles (e.g. the Amazon Echo™ and smart TVs), household goods (e.g. smart kitchen appliances and Nest™ utility meters), and security cameras are just a few of the more common IoT devices we (intentionally or unintentionally) interact with on a daily basis.

12. Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring) ("[A] person has a constitutionally protected reasonable expectation of privacy.").

13. *See generally* Alan F. Westin, *Privacy and Freedom*, 25 WASH. & LEE L. REV. 166 (1968).

14. ERIC A. FISCHER, CONG. RESEARCH SERV., R44227, THE INTERNET OF THINGS: FREQUENTLY ASKED QUESTIONS (2015).

15. Melissa W. Bailey, *Seduction by Technology: Why Consumers Opt out of Privacy by Buying into the Internet of Things*, 94 TEX. L. REV. 1023 (2016).

The value of these sorts of consumer-oriented IoT devices is fairly well understood by those who use them—convenience, safety, task automation, cost efficiency, and entertainment all contribute to the rise in IoT popularity.

On a larger scale, IoT technology will substantially contribute to a more integrated and functional social infrastructure,[16] promising ground-breaking developments in transportation, increases in industrial productivity, improved energy conservation, increased agricultural productivity and food supply, and improved community safety.[17] Estimates of the current total number of IoT devices vary, but it is clear that the number is going to skyrocket in the near future; one analytics firm projects that there will be over 26 billion connected devices by 2020,[18] while others place the projected total between 40.9 and 212 billion by the same year.[19] The economic value of the IoT is equally difficult to quantify. Estimates by the McKinsey Global Institute, taking into consideration the potential value of IoT technology across nine major settings, projects an annual economic value between $3.9 trillion - $11.1 trillion by 2025.[20] While this projection incorporates some degree of speculation with regard to industries like transportation, which relies on an assumption that there will be widespread implementation of IoT-enabled autonomous vehicles, one area that is already exploding in popularity is home goods and services, valued between $200–$350 billion annually by 2025.[21] Encompassing this estimate is a valuation of IoT-facilitated chore automation, energy management, and home security.[22] Consumer products will be the focal point of this note.

While the IoT promises exciting developments in all facets of society, "privacy and security concerns [are] growing at an unparalleled rate"[23] due

16. FISCHER, *supra* note 14.

17. Christian S. McMeley, *Protecting Consumer Privacy and Information in the Age of the Internet of Things*, 29 ANTITRUST 71, 72 (2014).

18. 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/#d4987661d091.

19. *See* McMeley, *supra* note 17, at 72; *see also* Comments of the Staff of the Fed. Trade Comm'ns Bureau of Consumer Protection, *In the Matter of the Internet of Things and Consumer Product Hazards,* No. CPSC-2018-007, (June 15, 2018) [hereinafter Consumer Protection Bureau Comments], https://www.ftc.gov/system/files/documents/advocacy_documents/comment-staff-federal-trade-commissions-bureau-consumer-protection-consumer-product-safety/p185404_ftc_staff_comment_to_the_consumer_product_safety_commission.pdf (estimating 55 billion IoT devices by 2025).

20. Manyika et al., *supra* note 11, at 2.

21. *Id.*

22. *Id.*

23. Williams, *supra* note 10, at 14.

to the rapid development and implementation of IoT devices. The privacy concerns implicated by IoT devices are numerous, yet often difficult to isolate and address. Many IoT devices directly collect sensitive personal information, including location data, financial information, and personal health information.[24] In some cases, this automatic, comprehensive data collection is advertised as a feature—for example, FitBits™ collect a significant amount of intimate information about users, including location data and personal information like "steps walked, calories burned, activity intensity, sleep [habits], and other health and fitness metrics."[25] However, like other IoT devices, the personal data collected by FitBits™ has the potential to be used for less-than-benign purposes, including discrimination by employers, insurers, and lenders.[26]

Additional privacy concerns stem from inferential capabilities and data aggregation: "The collection of personal information, habits, locations, and physical conditions over time . . . may allow an entity that has not directly collected sensitive information to infer it."[27] In other words, discrete data points collected by IoT devices can be combined with other sources of input to "present a deeply personal and startlingly complete picture of each of us . . . ."[28] Data aggregation is discussed further in Part II.D.

From a security standpoint, IoT devices pose tangible risks by, among other things, "1) [E]nabling unauthorized access and misuse of personal information; 2) facilitating attacks on other systems; and 3) creating safety risks."[29] No Internet-connected devices are immune from hacking, no matter how innocuous they appear. These security risks will be further explored in Part II.C.

Consumers of IoT products are generally "unaware of the full extent of the privacy that they are trading and to whom their privacy is being sold."[30] Both the consumers and the sellers are to blame for this unfortunate reality, although not necessarily in equal parts. Sellers tend to intentionally make it difficult for customers to inform themselves of how their data is collected and utilized. In particular, they often hide their

24. *Id.*

25. Nicole Chauriye, *Wearable Devices as Admissible Evidence: Technology is Killing Our Opportunity to Lie*, 24 CATH. U. J. L. & TECH. 495, 497 (2016).

26. *See* Ifeoma Ajunwa, Kate Crawford, & Jason Schultz, *Limitless Worker Surveillance*, 105 CAL. L. REV. 735 (2017); Scott R. Peppet, *Regulating the Internet of Things: First Steps Toward Managing Discrimination, Privacy, Security, and Consent*, 93 TEX. L. REV. 85, 118 (2014).

27. FED. TRADE COMM'N, FTC STAFF REPORT: INTERNET OF THINGS: PRIVACY & SECURITY IN A CONNECTED WORLD, 14 (Jan. 2015) [hereinafter FTC STAFF REPORT].

28. Edith Ramirez, Chairwoman, Fed. Trade Comm'n, Opening Remarks at the Federal Trade Commission Internet of Things Workshop (Nov. 19, 2013).

29. FTC STAFF REPORT, *supra* note 27, at 10.

30. Bailey, *supra* note 15, at 1034.

privacy policies or make them difficult to read.[31] Additionally, it is often in sellers' best interests to keep their data gathering practices as secretive and comprehensive as possible—consumers may not be happy that their personal data is being bought and sold without their knowledge, but personalized consumer data (facilitating highly targeted ads) is the 'new oil' amongst internet marketers in the severely under-regulated data brokerage industry.[32] On the other hand, the risks associated with IoT data collection are, at least in part, self-imposed consequences resulting from consumers' implicit or explicit valuation of the convenience of IoT products over the various concerns associated with their use.[33] For example, a consumer who installs a motion-activated security camera in their fenced-in backyard should not be surprised when it records them mowing the lawn. Regardless of fault, the main issue here is not that consumers are oblivious to the fact that IoT devices are gathering information, but rather they do not grasp the full extent of data collection and the implications of that collection regarding their privacy interests.

II. ISSUES IN IOT DATA COLLECTION

Each of the following sections are the sole subjects of several different studies and articles in the growing body of literature on the IoT. My intention here is merely to introduce each issue to highlight the diverse and unexpected privacy implications of everyday IoT devices, because they are all relevant to the theoretical discussion in Part IV.

A. Unavoidable & Comprehensive IoT Data Collection

IoT consumer products are a growing source of information for law enforcement investigators due to the comprehensive nature of their data collection processes. As one commenter puts it, the "ubiquitous devices can serve as a legion of witnesses, capturing our every move . . . ."[34] The CEO of Enlightened, a company that produces sensor-equipped LED light

31. Peppet, *supra* note 26, at 139–143 (highlighting the difficulty of locating privacy policies and manufacturers' usage of unclear, ambiguous language in policies).

32. *See* Paul Boutin, *The Secretive World of Selling Data About You*, NEWSWEEK (May 30, 2016), http://www.newsweek.com/secretive-world-selling-data-about-you-464789; Andrew Guthrie Ferguson, *The Internet of Things and the Fourth Amendment of Effects*, 104 CAL. L. REV. 805, 817 (2016) ("Mapping consumer interests at an extremely personal level has become a growing and quite lucrative business, with many big technology companies jumping into the field.").

33. *See generally* Bailey, *supra* note 15.

34. Justin Jouvenal, *Commit a Crime? Your Fitbit, Key Fob or Pacemaker Could Snitch on You*, CHICAGO TRIB. (Oct. 9, 2017, 7:48 PM), http://www.chicagotribune.com/news/nationworld/ct-FitBit™-key-fob-pacemaker-crime-20171009-story.html.

systems, stated: "We can literally tell you how every square foot is occupied every second of every day."[35] The aforementioned Bates case is just one of several recent cases highlighting the potential impact of unavoidable IoT data collection in the context of criminal prosecutions. For instance, in September 2016, an Ohio man claimed that a fire began in his home while he was sleeping. Suspecting arson, the police filed a search warrant to get data from his pacemaker: "Authorities said his heart rate and cardiac rhythms indicated the man was awake at the time he claimed he was sleeping. He was charged with arson and insurance fraud."[36]

In another recent case, a Connecticut man named Richard Dabate was found guilty of murdering his wife after "data from the home's 'alarm system, computers, cellphones, social media postings and [his wife's] FitBit™ [created] a timeline that contradicted [his] statements to police.'"[37] Dabate claimed that an intruder had chased his wife into the basement and shot her immediately after she returned home from an exercise class; however, after gathering data recorded on her FitBit™, detectives determined that "she had walked 1,217 feet after returning home from the exercise class, far more than the 125 feet it would take her to go from the chair in the garage to the basement in [Dabate's] telling of what happened."[38] As if that wasn't enough, "The FitBit™ also registered Connie moving roughly an hour after [Dabate] said she was killed before 9:10 a.m."[39]

While two of these three cases ultimately resulted in net positive outcomes—putting away a murderer and an arsonist—the means by which these convictions came about are troubling. Consider again the Bates case, in which the prosecution's 'key' piece of evidence was water usage data gathered from a pre-installed smart utility meter.[40] While seemingly innocuous, smart meter data "can reveal the activities and behavioral patterns of a household . . . . [T]he detailed information contained in smart meter data can provide police with infinitely more insight into people's homes."[41] Bates did not choose to install the meter and certainly did not voluntarily disclose the information contained therein, but nonetheless,

35. Immanuel Kim, *The Internet of Things: A Reality Check for Legal Professionals*, LAW PRACTICE TODAY (Jan. 14, 2016), https://www.lawpracticetoday.org/article/the-internet-of-things-a-reality-check-for-legal-professionals/.

36. *Id.*

37. Mary Ann Georgantopoulos, *A Fitbit Helped Police Arrest a Man for His Wife's Murder*, BUZZFEED NEWS (Apr. 25, 2017, 3:37 PM), https://www.buzzfeed.com/maryanngeorgantopoulos/FitBit-murder?utm_term=.cgeEejG#.pm05rJx.

38. *Id.*

39. *Id.*

40. Wang, *supra* note 5.

41. Natasha H. Duarte, *The Home Out of Context: The Post-Riley Fourth Amendment and Law Enforcement Collection of Smart Meter Data*, 93 N.C. L. REV. 1140, 1140–41 (2015).

that data eventually sealed his fate (that is, of course, until the prosecution was dismissed).[42] Similarly, the pacemaker case suggests that individuals with serious heart problems face the unnerving prospect of the only piece of equipment keeping them alive recording discoverable evidence 24/7.

These concerns will increase exponentially in coming years as IoT devices continue to grow in popularity and diversity. For instance, Amazon announced its Echo Dot™ (mini Echo speakers) was its best-selling product of the 2017 holiday season, and the 'Alexa' phone app (the Echo's primary user interface) was briefly the most downloaded application on Apple's App Store.[43] Whether an individual owns a particular product or not, exposure to IoT device data collection in both public and private settings is becoming unavoidable as they seamlessly integrate into our social infrastructure.

B. Lack of Notice of IoT Data Collection

A major part of the problem with pervasive, unavoidable IoT data collection is the lack of transparency on the part of those doing the collecting. Manufacturers of IoT products have little interest in disclosing to their consumers just how much data manufacturers are collecting about consumers—nor, in most instances, are there any federal regulations explicitly requiring manufacturers to do so.[44] In 2015, the FTC announced it would not require consumer notification practices "before collecting and using consumer data for practices that are consistent with the context of a transaction or the company's relationship with the consumer."[45] The FTC report acknowledged that consumer notice and choice of privacy settings are important,[46] but it did not want to stifle the growth and development of IoT technology, while also noting: "these data uses are generally consistent with consumers' reasonable expectations."[47]

This particular conclusion stands in stark contrast to a statement made by Former FTC Commissioner Julie Brill just a few months earlier:

---

42. Neal, *supra* note 9.

43. Raymond Wong, *Amazon's Echo Dot and Alexa Voice Assistant Ruled this Holiday Season*, MASHABLE (Dec. 27, 2017), http://mashable.com/2017/12/27/amazon-echo-dot-alexa-smart-home-top-holiday-2017-gift/#.fj3GD3Kxsqp.

44. Bailey, *supra* note 15, at 1032 ("Furthermore, there does not currently exist federal regulation requiring manufacturers to notify consumers about when or what types of data are collected when the collected information is used for a purpose consistent with the transaction.").

45. FTC STAFF REPORT, *supra* note 27, at 40.

46. *See* Kim, *supra* note 35 ("The FTC urges industry-initiative self-regulations of the IoT implementations. The recommendations include: 1) a privacy-by-design approach; 2) minimized collection and retention of consumer data; 3) notice of data use and sharing; and 4) consumer's choice on data use.").

47. Bailey, *supra* note 15, at 1032.

> On the Internet of Things, consumers are going to start having devices . . . that [are] connected and sending information to a number of different entities, and the consumer may not even realize that they have a connected device or that the thing that they're using is collecting information about them.[48]

In effect, the FTC simultaneously acknowledges that consumers may not realize they are using an IoT device (let alone one that is collecting and sending their data to a third party), while also asserting that when consumers use said devices, companies are not under any obligation to provide notice of data collection if the consumer could 'reasonably expect' that the data collection was being used for purposes 'consistent with the context of the transaction.'[49] The effect of the FTC's laissez-faire approach to consumer notice provisions is that manufacturers can generally choose what information they disclose about their data collection practices. Consumers are usually bound to the manufacturer's terms via contracts of adhesion, meaning as soon as consumers start using a device, they are presumed to have consented to the terms of use.[50] In other words, consumers are presented with a 'choice,' but that choice is little more than the manufacturer stating "take it or leave it"—either accept the terms of use, or don't use the product.

Even if a consumer *wants* to find out the kinds of data the manufacturer is collecting, they will face several obstacles. First, given the small physical size of most consumer-oriented IoT devices, manufacturers often cannot display privacy notices on the device or packaging itself.[51] Accordingly, if consumers want any information, they have to seek out the manufacturer's privacy policy from some external source (often the manufacturer's website), a process Noah Peppet suggests is easier said than done: "[F]or several of the products reviewed it was extremely difficult to even locate a relevant privacy policy."[52] In addition, the terms of these privacy policies are often ambiguous and unclear, utilizing differing definitions of "personal information" across devices and consequently misleading consumers about how their data is shared or sold to third parties.[53] Manufacturers maintain wide, unilateral discretion with

48. Julie Brill, Comm'r, Fed. Trade Comm'n, Address at the Silicon Flatirons Conference: The New Frontiers of Privacy Harm (Jan. 17, 2014).

49. The FTC does, however, recommend data minimization practices (i.e. limiting the quantity of data collection and the period of data retention) due to the "increased risk that the data will be used in a way that departs from consumers' reasonable expectations." FTC STAFF REPORT, *supra* note 27, at 35.

50. Bailey, *supra* note 15, at 1033.

51. Peppet, *supra* note 26, at 140.

52. *Id.* at 141.

53. *Id.* at 142.

regard to the "third parties" or "partners" with whom they share collected data, and consumers generally have no way of even finding out who those third parties may be, let alone assess their data security practices or how they process and utilize the personal data they eventually receive.

These practices can have significant implications for consumer privacy interests. For example, in 2015, Samsung Group came under fire after an anonymous internet user pointed out that the privacy policy for the popular Samsung SmartTV™, a television with a built-in Voice Recognition feature, contained an eerie disclaimer: "Please be aware that if your spoken words include personal or other sensitive information, that information will be among the data captured and transmitted to a third party through your use of Voice Recognition."[54] To put that disclaimer in context, "[t]hat means if you decide to go 'live in the future' and turn on *Game of Thrones* with just your voice, the TV will translate that speech to text and whatever else you say and send the data to third-party companies."[55] The privacy policy goes on to state: "Samsung is not responsible for these providers' privacy or security practices," distancing itself from any accountability for the third party's use of their consumers' potentially private information.

Fortunately, the FTC has since taken note of questionable data collection practices in the smart TV industry. In 2017, VIZIO, Inc. settled[56] with the FTC after the FTC alleged VIZIO installed software on its TVs which collected individualized, second-by-second viewership data without notifying its users.[57] Per the terms of the FTC consent decree, VIZIO agreed to implement notice and consent procedures, along with a data deletion policy and a comprehensive privacy program.[58]

---

54. Darren Orf, *Samsung's SmartTV Privacy Policy Raises Accusations of Digital Spying*, GIZMODO (Feb. 8, 2015, 2:30 PM), https://gizmodo.com/samsungs-smart-tv-privacy-policy-raises-accusations-of-1684534051.

55. *Id.*

56. Stipulated Order for Permanent Injunction & Monetary Judgment, FTC v. Vizio, Inc., No. 2:17-cv-00758 (D.N.J. Feb. 6, 2017) [hereinafter FTC Stipulated Order].

57. In addition to selling TVs without notifying consumers of the built-in "automated content recognition" (ACR) data collection software, VIZIO remotely installed the ACR software on previously-sold TVs, again without consumer notification. VIZIO then sold the viewing history to various third parties, in part to facilitate targeted advertising to particular consumers based on their television viewing data. Complaint for Permanent Injunction & Other Equitable and Monetary Relief, FTC v. Vizio, Inc., No. 2:17-cv-00758, 4–5 (D.N.J. Feb. 6, 2017).

58. FTC Stipulated Order, *supra* note 56, at 4 ("[P]rior to collecting any Viewing Data, [VIZIO] must: Prominently disclose to the consumer, separate and apart from any 'privacy policy,' 'terms of use' page, or other similar document, (1) the types of Viewing Data that will be collected and used, (2) the types of Viewing Data that will be shared with third parties; (3) the identity or specific categories of such third parties; and (4) all purposes for Defendants' sharing of such information.").

Although the *VIZIO* enforcement action may be a signal that the FTC is slowly shifting its stance on data collection notice requirements, it remains to be seen whether the decree will have a demonstrable impact in the broader IoT industry. VIZIO's conduct was particularly egregious, and complex data processing relationships can often make it difficult to determine exactly where the burden of consumer notice should lay. For example, Amazon is notably secretive about the full parameters of its data collection practices, and is currently working with a number of third-party companies (including home security system sellers, toy manufacturers, and health trackers) to incorporate Alexa into their IoT products.[59] Amazon maintains that their devices do not have the technical capacity to record and store any ambient conversations without first triggering the devices to listen, but regardless, everything intentionally said to the device—purchases, questions, messages to other Echo™ users, reminders, alarms, etc.—are recorded and stored on the users' Amazon account.[60] With each new third party processor comes an added layer of complication, and an added level of practical difficulty in effectuating adequate consumer notice. Is Amazon obligated to notify users of *any* third-party products incorporating Alexa technology every time that product collects consumer data? Or should the burden fall on the third-party product manufacturer? As new IoT technologies proliferate and interconnect, these questions will become more and more difficult to answer.[61]

C. Inadequate Data Security

The FTC identifies three categorical security risks posed by IoT devices.[62] The first is unauthorized access to IoT devices and misuse of personal information.[63] Poor security in IoT devices and data transactions, both on the consumer and server side, can enable intruders to compromise user credentials or otherwise hack into the device in order to gather stored

---

59. Electronic Privacy Information Center, *EPIC Letter to the Attorney General and the FTC Chairwoman* (July 10, 2015), https://epic.org/privacy/internet/ftc/EPIC-Letter-FTC-AG-Always-On.pdf.

60. Janko Roettgers, *Relax: Your Amazon Echo Isn't Recording Everything You Say*, VARIETY (Dec. 27, 2016, 3:01 PM), http://variety.com/2016/digital/news/amazon-echo-spying-privacy-1201948926/.

61. FTC STAFF REPORT, *supra* note 27, at 22.

> As one participant observed, when "a bunch of different sensors on a bunch of different devices, on your home, your car, your body . . . are measuring all sorts of things," it would be burdensome both for the company to provide notice and choice, and for the consumer to exercise such choice every time information was reported.

Id.

62. *See* FTC STAFF REPORT, *supra* note 27, at 10.

63. *Id.* at 10–11.

or transmitted information.[64] This problem is exacerbated if the device stores or transmits financial information or personally identifiable information, as both can be used to facilitate further identity theft or fraud.[65]

Some companies seek to protect consumers by "de-identifying" user data, or processing and storing data without revealing the identity of the individual source.[66] However, the effectiveness of de-identification in the IoT sphere questionable: "[D]e-identification is not a perfect solution because in most of the de-identified datasets, the information can be *re*-identified."[67] As Peppet asserts, "Preliminary research suggests that robust anonymization of Internet of Things data is extremely difficult to achieve, or, put differently, that re-identification is far easier than expected."[68]While the actual risk and efficacy of re-identification techniques are still being debated,[69] IoT devices often collect "high-dimensional data"[70] about user behaviors, facilitating the ease of any targeted attempts at re-identification—particularly when combined with publicly-available information.[71]

The other major security concern implicated by IoT devices is the potential for malicious intrusion and criminal misuse of the devices. IoT

---

64. Consumer Protection Comments, *surpa* note 19, at 7.

> The FTC has also recommended that companies consider risks at the point where a service communicates with an IoT device, such as the interface between the device and the cloud. Security experts have long warned against attack vectors such as cross-site scripting attacks, where malicious scripts are injected into otherwise trusted websites, and cross-site request forgery attacks, where unauthorized commands are sent from a user the website trusts.

Id.

65. Mario Ballano Barcena et al., *Security Response, How Safe is Your Quantified Self?*, SYMANTEC (Aug. 11, 2014, 12:00 PM), http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/how-safe-is-your-quantified-self.pdf.

66. Ann Cavoukian & Daniel Castro, *Big Data and Innovation, Setting the Record Straight: De-identification Does Work* 1 (June 2014), http://www2.itif.org/2014-big-data-deidentification.pdf.

67. Bailey, *supra* note 15, at 1030.

68. Peppet, *supra* note 26, at 130.

69. *Compare* Cavoukian & Castro, *supra* note 66; *with* Arvind Narayana & Edward Felten, *No Silver Bullet: De-identification Still Doesn't Work* (July 9, 2014), http://randomwalker.info/publications/no-silver-bullet-de-identification.pdf.

70. "High-dimensional data" is defined as a dataset consisting of numerous data points about each individual such that each individual record is likely to be unique. One example is mobility data collected periodically by cell phone providers. Each time a cellphone connects with a cell phone tower and transmits its location, it adds another data point to the users' dataset. In this context, re-identification would consist of analyzing as few as two discrete location data points to identify the user—for instance, by determining the location of their home and place of work. Narayana & Felten, *supra* note 69, at 4.

71. Cavoukian & Castro, *supra* note 66, at 3 ("[I]t is admittedly very difficult to de-identify mobility traces [and high-dimensional data] . . . due to their high degree of uniqueness. In the case of high-dimensional data, additional arrangements may need to be pursued, such as making the data available to researchers only under tightly restricted legal agreements.").

devices may create hazards through the loss of a critical safety function, loss of connectivity, or degradation of data integrity.[72] Additionally, consumer IoT devices are susceptible to intrusion by any number of well-known methods (failing to change default passwords, inadequate firewall protection, phishing attacks, etc.) or more sophisticated means (coordinated DDoS attacks, brute force hacking, etc.).[73] Even if the network is well-protected, specific devices may not be; many IoT devices share similar characteristics to WIFI routers, specifically with regard to default usernames and passwords, and individual devices can be targeted with startling precision and concerning results. For example, "[In August 2013,] a creepy dude hacked into a Houston family's Web-connected baby monitor to call a 2-year-old a 'little slut.' The family was using a 'high quality video and audio' camera made by China-based Foscam."[74] While hacking into baby monitors is certainly on the creepier end of the spectrum, the implications could be life threatening as well: "[D]octors for former Vice President Dick Cheney ordered the wireless functionality of his heart implant disabled due to fears it might be hacked in an assassination attempt."[75] The U.S. Food and Drug Association now includes cybersecurity protection as one of several evaluation criteria for approval of medical devices.[76]

---

72. For instance:

> [A] car's braking systems might fail when infected with malware, carbon monoxide detectors or fire alarms might stop working with the loss of connectivity, and corrupted or inaccurate data on a medical device might pose health risks to a user of the device. Consumers' physical safety could also be at risk if an intruder had access to a connected lock, garage door, or burglar alarm.

Consumer Protection Bureau Comments, *supra* note 19, at 2.

73. For example:

> Hackers used the Mirai botnet—composed of IoT devices, such as IP cameras and routers, infected with malicious software—to engage in a distributed denial of service ("DDoS") attack of unprotected residential building management systems in Finland. By blocking Internet access, hackers sent these connected management systems into an endless cycle of rebooting, leaving apartment residents with no central heating in the middle of winter. Also, earlier this year, researchers discovered vulnerabilities in Internet-connected gas station pumps that, when remotely accessed, would allow hackers not only to steal credit card information but also change the temperature and pressure in gas tanks, potentially causing explosions.

Id. at 3; *see also* G.G. Veerendra, *Hacking Internet of Things (IoT): A Case Study on DTH Vulnerabilities,* SECPOD https://www.secpod.com/resource/whitepapers/Hacking-IoT-A-Case-Study-on-Tata-Sky-DTH-Vulnerabilities.pdf; *The 5 Worst Examples of IoT Hacking and Vulnerabilities in Recorded History*, IOT FOR ALL (May 10, 2017), https://www.iotforall.com/5-worst-iot-hacking-vulnerabilities/.

74. Kashmir Hill, Baby Monitor Hack Could Happen to 40,000 Other Foscam Users, Forbes (Aug. 27, 2013), https://www.forbes.com/sites/kashmirhill/2013/08/27/baby-monitor-hack-could-happen-to-40000-other-foscam-users/#28c6069758b5.

75. Herbert B. Jr. Dixon, *The Wonderful and Scary Internet of Things*, 56 JUDGES J. 36, 37 (2017).

76. *Id.*

Several federal and state-level regulations codify requirements to reasonably protect certain information, including the Fair Credit Reporting Act (FCRA), Children's Online Privacy Protection Act (COPPA), Health Insurance Portability and Accountability Act (HIPAA), Electronic Signatures in Global and National Commerce Act, and the Fair and Accurate Credit Transactions Act (FACTA).[77] However, none of these statutory schemes specifically cover IoT data. Instead, the existing protections are generally limited to specific content (e.g., FCRA only protects personally identifiable credit report information[78]), or specific types of data processors (e.g., HIPAA only applies to entities that electronically process health insurance information[79]). Even where IoT data could reasonably fall within the parameters of a statute, rigid statutory schemes fail to account for the unique nature of IoT data collection. For example, FitBits™ collect everything from an individuals' daily running routes, to eating habits, sleeping patterns, symptom searches, and cadence of a person's walk or run—unquestionably personal health information—but FitBit is not covered by HIPAA because it is not a "covered entity": "[M]uch consumer-generated health information created from apps or devices falls outside the reach of HIPAA and the Health Information Technology for Economic and Clinical Health Act (HITECH)."[80]

While statutory schemes are largely ineffective, some federal agencies are attempting to safeguard IoT data from malicious breaches by imposing liability on IoT manufacturers. As previously noted, the FTC is "empowered and directed to prevent [certain] persons . . . from using unfair methods of competition in or affecting commerce and unfair or deceptive acts or practices in or affecting commerce."[81] The FTC's authority to pursue "unfair or deceptive acts" appears to be one of the primary vehicles through which the federal government will attempt to hold IoT manufacturers accountable: "With the vast amount of data generated by the Internet of Things and the unending string of data breaches, the FTC has increased the use of its Section 5 authority to ensure businesses are implementing 'reasonable' security measures."[82] The FTC

77. McMeley, *supra* note 17, at 76.

78. 16 C.F.R. § 682.3(a) (2004) ("Any person who maintains or otherwise possesses consumer information for a business purpose must properly dispose of such information by taking reasonable measures to protect against unauthorized access to or use of the information in connection with its disposal.").

79. 45 C.F.R. § 160.102 (2003) (providing that the HIPAA Security Rule applies only to the following entities: health plan, health care clearinghouse, health care provider who transmits any health information in electronic form, and business associates).

80. McMeley, *supra* note 17, at 74.

81. 15 U.S.C. § 45(a)(2) (2006).

82. McMeley, *supra* note 17, at 74.

has already applied its Section 5 authority in one IoT-related data breach action signaling to other manufacturers that they may be on the hook for inadequate security measures.[83] Regardless, as more IoT products (and producers) flood the market, the potential for breaches inevitably rises—maintaining adequate data security is a continuous process, and the IoT is no exception.

D. Potential for Discrimination & Improper Evidentiary Inferences

While the aforementioned *Dabate* case demonstrates some of the positive, pragmatic capabilities of IoT data in facilitating criminal prosecutions, one concerning implication associated with IoT data is the potential for improper and unfair evidentiary inferences. For example, Nichole Chauriye suggests IoT data was improperly admitted in *Commonwealth v. Risley*.[84] In 2015, a woman named Jeannine Risley reported that she was sexually assaulted by a masked intruder while staying overnight at her boss' home.[85] During the subsequent investigation, the police found Risley's FitBit™ lying in the hallway. Upon the investigators' request, Risley provided her FitBit's™ password as well as her consent to search and collect the electronically stored data.[86] After reviewing the data, the police concluded: "[T]he data retrieved from the device indicated that she may have been walking around at the time of the alleged attack."[87] This contradicted her claim that she was woken from bed by the attacker. Risley was later charged with making false statements, and the FitBit™ data was introduced as proof that she had lied about the attack.[88] Chauriye suggests that the introduction of the FitBit™ data was prejudicial to Risley, and perhaps unconstitutional:

---

83. In re Trendnet, Inc., No. 122-3090, 2013 WL 4858250 (F.T.C. Sept. 3, 2013). In 2013, the FTC filed a complaint under Section 5 of 15 U.S.C. § 45(a) against TRENDnet, a company which sold sensor-equipped IP security cameras. The cameras were accessible via remote log-in, allowing users to access live feeds. The FTC alleged, *inter alia*, that TRENDnet failed to establish reasonable security measures, specifically by transmitting and storing user login credentials in clear, readable text over the Internet. Hackers exploited the vulnerability to gain access to 700+ camera feeds. The FTC settled with TRENDnet, imposing substantial notification, reporting, and security requirements on the company.

84. Chauriye, *supra* note 25, at 496 (citing Commonwealth v. Risley, Criminal Docket: CP-36-CR-0002937-2015 (Lancaster Cty., Pa, printed Nov. 16, 2015)).

85. Sophie Kleeman, *Woman Charged with False Reporting After Her FitBit Contradicted Her Rape Claim*, MIC NEWS (June 25, 2015), http://bit.ly/1SNAeLY.

86. Chauriye, *supra* note 25, at 510.

87. *Id.* at 509–10.

88. *Id.* at 510.

While the FitBit™ contradicts her statements; it does not prove that she lied. The events of that night could still have happened as she claims. The fact is that FitBits™, and other wearable technology, log data in certain time increments, but fail to capture the exact details of what happens during a particular time. It is for this reason that allowing such data from wearable technology to be admitted as evidence is severely flawed and may cause an unfair bias against the owner of the technology.[89]

This case poses a troubling dilemma. On one hand, if Risley *did* fabricate the rape claim, as the evidence tends to suggest, then the FitBit™ data is valuable to the extent that it supports her criminal prosecution. On the other hand, if the attack actually happened but Risley simply forgot or misremembered some of the details, or alternatively, if the data was faulty or misleading,[90] then the use of the FitBit™ data becomes a kind of malicious form of victim-blaming, leading to criminal charges stemming solely from Risley's trivially inaccurate recollection of a deeply traumatic event.[91]

Criminal prosecutions are not the only ways in which IoT data can be used against consumers to their detriment. Another growing area of concern is IoT-facilitated discrimination in the insurer-insured and creditor-debtor contexts:

> If the [IoT] creates many new data sources from which unexpected inferences can be drawn, and if those inferences are used by economic actors to make decisions, one can immediately see the possibility of seemingly innocuous data being used as a surrogate for racial or other forms of illegal discrimination.[92]

Creditors may not actually know an applicant's race, but they could easily guess that race based on "where and how a person drives, where and how that person lives, or a variety of other habits, behaviors, and characteristics revealed by analysis of data from a myriad of IoT devices."[93] Aggregated IoT data can therefore be used as a proxy for otherwise impermissible racial or class-based discrimination, even if those impermissible factors are never actually referenced. In the insurer-insured context, the use of IoT data in pricing determinations is already being implemented—car insurance companies allow drivers to travel with

89. *Id.*

90. Katherine E. Vinez, *The Admissibility of Data Collected from Wearable Devices*, 4 STETSON J. ADVOC. & L. 24 (2017).

91. Chauriye, *supra* note 25, at 511.

92. Peppet, *supra* note 26, at 123–24.

93. *Id.* at 124.

devices that track speed and location data, and while the service is purported to help lower insurance premiums, it can just as easily be used to raise insurance rates if the device records any instances of aggressive driving.[94]

IoT data also has the potential to be used for discriminatory purposes in employment contexts. FitBit's™ "wellness program" service for employers is one potential example. Through these programs, employers can establish company-wide health milestones or fitness goals for their employees to reach.[95] Employers may then either offer FitBits to employees (or permit employees to opt in), providing incentives to employees who hit the established metrics.[96] While there may be beneficial individual and company-wide results if utilized properly, "these data carry the inherent risk of 'reveal[ing] physical disabilities, illnesses, or conditions like pregnancy,' and some employers have already fired employees 'who engage in behavior likely to raise the employer's health insurance costs.'"[97] Accordingly, employees are faced with a lose-lose situation—choose *not* to participate and lose out on incentives (in addition to possible social ostracization), or opt in to the program and run the risk of private or latent health issues coming to light and adversely impacting employment status. Again, while wearable technologies undoubtedly have beneficial effects for millions of active users, a certain degree of trust must necessarily be placed in the companies collecting the data: "Consumer privacy experts have already expressed concern that the information collected by companies like FitBit is so detailed that it could 'enable companies to do everything from accurately guessing your credit rating to pricing an insurance premium.'"[98]

Successfully stating an actionable claim of discrimination based on IoT data aggregation would be next to impossible—not only is it becoming increasingly difficult to ascertain what, where, and how personal data is being collected, but neither traditional antidiscrimination laws nor data processing regulations like FRCA (to be discussed in Part III) prohibit employers, lenders, insurers, creditors, and other entities from utilizing IoT data in formulating their decisions.[99]

---

94. Bailey, *supra* note 15, at 1031.
95. *See id.* at 1030–31.
96. *Id.*
97. *Id.*
98. Chauriye, *supra* note 25, at 496.
99. Peppet, *supra* note 26, at 128; *see also* Ifeoma Ajunwa, Kate Crawford, & Jason Schultz, *Limitless Worker Surveillance,* 105 CAL. L. REV. 735 (2017) (proposing three statutory frameworks for addressing legal deficiencies in employee privacy protections).

III. CURRENT LEGAL STANDARDS GOVERNING THE ADMISSIBILITY OF IOT DATA

To review, I have provided an abridged explanation of some of the more significant privacy issues associated with individual and collective use of IoT products. While the aforementioned issues are tangible concerns, IoT products are here to stay—and rightfully so. By any objective measure, the economic, technological, and societal value of IoT products (both current and predictive) is simply too great to prudently hamper via excessive governmental regulation.[100] However, while *technical* issues like inadequate data or device security may be fixable by taking concrete, tangible precautions,[101] I would argue that the IoT poses irreconcilable *philosophical* issues in light of long-standing norms in the diverse body of privacy theory. The next sections will explore this area in two parts; in Part III, by outlining the current legal framework surrounding the IoT and the evidentiary admissibility of IoT data, and in Part IV, by explaining how the current standards are, at the very least, inconsistent with the philosophical underpinnings of privacy jurisprudence.

A. IoT Data as Evidence

The previous sections, and specifically the *Bates*, *Dabate*, and *Risley* cases, provide snapshots of the potential evidentiary value of IoT data. In each of those cases, police found a device near the scene of the crime, filed a subpoena for the device's electronically stored data with the third-party processor, and, once the request was granted, utilized the data in the subsequent prosecution. The standards for accessing stored IoT data under current federal regulations are less stringent than those for acquiring a warrant. The Stored Communications Act, enacted as Title II of the Electronic Communications Privacy Act of 1986 (ECPA),[102] provides several means by which police can compel the disclosure of certain electronically stored information (ESI). If the requested ESI is less than 180 days old, a formal warrant supported by probable cause is required.[103] If, however, the ESI is more than 180 days old, police can access the data by filing a formal warrant, filing an administrative subpoena, or by requesting the ESI through a court order.[104] Both of the latter two options

100. *See* Duarte, *supra* note 41.

101. *See, e.g.*, FED. TRADE COMM'N, CAREFUL CONNECTIONS: BUILDING SECURITY IN THE INTERNET OF THINGS (2015).

102. 18 U.S.C. §§ 2701–10 (2018).

103. 18 U.S.C. § 2703(a) (2018).

104. 18 U.S.C. § 2703(b) (2018).

require a lower burden of proof than a formal warrant; where the warrant requires a showing of probable cause, the administrative subpoena and court order merely require the police to show that there are reasonable grounds to believe that the information requested is 'relevant and material' to an ongoing criminal investigation.[105] There are typically some logistical hurdles to overcome with regard to the collection and admissibility of ESI under the Federal Rules of Evidence, namely establishing the relevancy of ESI, assessing its accuracy, and authenticating the data.[106]

Perhaps the most contentious evidentiary consideration is establishing the reliability of ESI, particularly in the context of ESI produced by IoT devices. Some scholars assert that data gathered by IoT devices is almost always going to be reliable, as sensors simply record inputs and transmit the information as they are programmed to do.[107] For them, the bigger problem is the *inferences* that can be drawn from the collected data, particularly when those inferences are for discriminatory or prejudicial purposes.[108] This is certainly true with devices like smart utility meters and fixed GPS location trackers in cars—for example, the fact that Bates used 140 gallons of water between 1:00 and 3:00A.M. is an objectively verifiable fact which the meter accurately recorded, but the troubling issue is that police attempted to frame the water usage data as evidence of a cover-up in order to support their (allegedly falsified) theory of the case.

On the other hand, others argue that IoT devices are inherently unreliable, and gathered data should only be used in limited circumstances to supplement, dispute, and rarely (if ever) to replace witness testimony.[109] Any number of occurrences could make IoT data unreliable. The sensor itself may make a technical error, or the collected data may become

---

105. The statute provides:

> A court order for disclosure under subsection (b) or (c) may be issued by any court that is a court of competent jurisdiction and shall issue only if the governmental entity offers specific and articulable facts showing that there are reasonable grounds to believe that the contents of a wire or electronic communication, or the records or other information sought, are relevant and material to an ongoing criminal investigation.

18 U.S.C. § 2703(d) (2018).

106. *See generally* Michael Arnold & Dennis R. Kiker, *The Big Data Collection Problem of Little Mobile Devices*, 21 RICH. J.L. & TECH. 10 (2015); Neda Shakoori, *Wearables: Your Next Trial Witness?* S.F. DAILY J. (Dec. 10, 2014), https://www.mcmanislaw.com/Templates/media/files/PDFs/McManis-Faulkner-DJ-12-10-14.pdf; Katherine E. Vinez, *The Admissibility of Data Collected from Wearable Devices*, 4 STETSON J. ADVOC. & L. 1 (2017).

107. Peppet, *supra* note 26, at 128 ("Accuracy, however, is really not the problem with Internet of Things sensor data. One's FitBit, driving, or smart home sensor data are inherently accurate—there is little to challenge.").

108. *Id*.

109. Shakoori, *supra* note 106 ("With the potentially inaccurate or incomplete narrative of a user's activities, it seems the use of wearable-generated data may be best served when supplemented with a more traditional form of evidence, testimony from the user or witnesses, such as the user's medical doctor.").

corrupted and degrade in accuracy over time.[110] Alternatively, devices like FitBits™ may inaccurately assess input data and record something that did not actually happen: "A wearable device could log a user as having walked three miles, when the user was actually just shuffling his feet back and forth at his workstation."[111] Inaccurate records such as these could have major implications in the future with regard to insurance claims and other proceedings where FitBit™ data is sought, and we have already seen at least one contentious case involving potentially unreliable data—commenters still debate the veracity and reliability of the FitBit™ data used in the *Risley* case.[112]

B. The Constitutionality of IoT Data Collection

The constitutional questions surrounding the collection and use of IoT data are equally as unsettled. Most prominent among these questions is how the IoT fits within the existing standards for searches and seizures under the Fourth Amendment.[113] In *Katz v. United States*[114], decided in 1967, the Supreme Court recognized that an individual's right to freedom from unwarranted governmental searches and seizures depends on that individual's reasonable expectation of privacy. Justice Harlan's concurring opinion in *Katz* established what has since become known as the reasonable expectation standard, now utilized to assess whether a search occurs under the meaning of the Fourth Amendment: "[T]here is a twofold requirement, first that a person have exhibited an actual (subjective) expectation of privacy and second, that the expectation be one that society is prepared to recognize as 'reasonable.'"[115] In effect, the reasonable expectation standard turns on *societal*, rather than individual expectations—any individual bringing a Fourth Amendment challenge can claim that they subjectively believed their communications were private—thus the standard is theoretically malleable and capable of adjustment by the courts according to shifting societal norms and expectations.[116]

---

110. Consumer Protection Bureau Comments, *supra* note 19, at 2 (citing CONSUMER PROD. SAFETY COMM'N, POTENTIAL HAZARDS ASSOCIATED WITH EMERGING AND FUTURE TECHNOLOGIES, 16 (Jan. 18, 2017)).

111. *Id.*

112. *Compare* Chauriye, *supra* note 25*, with* Vinez, *supra* note 90.

113. U.S. CONST. amend. IV.

114. Katz v. United States, 389 U.S. 347 (1967) (holding that the defendant exhibited a reasonable expectation of privacy in his conversations while in a closed telephone booth, such that a government-planted listening device in the booth violated his Fourth Amendment rights).

115. *Id*. at 361.

116. Orin S. Kerr, *An Equilibrium-Adjustment Theory of the Fourth Amendment*, HARV. L. REV. 482 (2011) ("When changing technology or societal practice expands police power, threatening civil liberties, courts can tighten Fourth Amendment rules to restore the status quo. The converse is

The *Katz* decision and the reasonable expectation standard superseded the Trespass Doctrine, the prevailing privacy standard established forty years prior to *Katz* in *Olmstead v. United States*[117] Under the Trespass Doctrine, a search under the Fourth Amendment only took place if the government physically trespassed on an individual's protected property interest. If there was no physical trespass by the police or a particular surveillance device, then there was no technical "search." However, the Supreme Court recently evoked the Trespass Doctrine in *United States v. Jones*,[118] holding that a GPS device physically planted on the defendant's car, used to monitor his location for several weeks, constituted a search under the Fourth Amendment. Rather than decide the case based on the *Katz* reasonable expectation standard, the majority took a very narrow approach to the issue, effectively deciding the case based on the physical intrusion alone.[119]

In *Jones*, Justice Sotomayor authored an influential concurring opinion in which she criticized the majority for punting on the issue of whether the surveillance via the GPS tracker itself constituted an unreasonable search, while also expressing concern about the possibility of data aggregation revealing more about an individual through inferential connections than the initial surveillance alone might suggest possible: "I would ask whether people reasonably expect that their movements will be recorded and aggregated in a manner that enables the Government to ascertain, more or less at will, their political and religious beliefs, sexual habits, and so on."[120] Sotomayor presciently asserted: "GPS monitoring generates a precise, comprehensive record of a person's public movements that reflects a wealth of detail about her familial, political, professional, religious, and sexual associations."[121] While Sotomayor's argument spoke specifically to GPS trackers, the device in question could just as easily be replaced by any number of IoT devices discussed in this note—FitBits™, Amazon Echos™, and even smart utility meters all have the capability to generate "comprehensive records" of our daily lives. However, because

---

true, as well. When changing technology or social practice restricts police power, threatening public safety, courts can loosen Fourth Amendment rules to achieve the same goal.").

117. Olmstead v. United States, 277 U.S. 438 (1928) (holding that a search and seizure under the Fourth Amendment did not occur where the government physically placed wiretaps on two of the defendant's phone lines because the taps were situated beyond the limits of his property).

118. United States v. Jones, 565 U.S. 400 (2012).

119. *Id*. at 404–05 ("We hold that the Government's installation of a GPS device on a target's vehicle, and its use of that device to monitor the vehicle's movements, constitutes a 'search.' It is important to be clear about what occurred in this case: The Government physically occupied private property for the purpose of obtaining information. We have no doubt that such a physical intrusion would have been considered a 'search' within the meaning of the Fourth Amendment when it was adopted.").

120. *Id.* at 416.

121. *Id.* at 415.

the Court declined to conclusively hold that comprehensive surveillance by means of data aggregation constitutes an unreasonable search under the *Katz*, Sotomayor's concurrence is little more than an artful articulation of a problem that will only be exacerbated by IoT technology.

The last major doctrinal issue in the relationship between the IoT and the Fourth Amendment concerns the Third Party Doctrine. First established in *United States v. Miller*,[122] the Third Party Doctrine maintains that individuals do not have a reasonable expectation of privacy in information voluntarily disclosed to a third party, thus a warrant supported by probable cause is generally not required to obtain information held by third parties.[123] In the IoT context, this means that when an individual voluntarily interacts with a device and that interaction is transmitted to a third party company for processing, the individual theoretically relinquishes any expectation of privacy they had in the disclosed information. Consequently, where direct, contemporaneous police surveillance of an individual via their IoT devices may implicate the Fourth Amendment's reasonable expectation standard, simply gathering the same data after the fact directly from the third party company would not.[124] As of yet, there are no explicit protections for IoT device information under existing constitutional law, thus traditional third party rules apply.[125]

There is a possibility this may change in the future, however. The Supreme Court recently declined to extend the Third Party Doctrine to historical location data gathered by cellphone towers.[126] In *Carpenter*, the Court recognized that "historical cell-site records present even greater privacy concerns than the GPS monitoring of a vehicle we considered in *Jones*,"[127] thus a warrant is required to obtain location records from cellphone providers. Chief Justice Roberts opined that the location data gathered by cellphone towers is comprehensive in scope and ubiquitous for all cellphone users, thus it is not comparable to the sort of limited information at issue in typical third-party cases: "There is a world of difference between the limited types of personal information addressed in *Smith* and *Miller* and the exhaustive chronicle of location information

122. United States v. Miller, 425 U.S. 435 (1976).

123. Orin S. Kerr, *The Case for the Third-Party Doctrine*, 107 MICH. L. REV. 561, 563–64 (2009).

124. Andrew Guthrie Ferguson, *The Internet of Things and the Fourth Amendment of Effects*, 104 CAL. L. REV. 805, 840 (2016).

125. *Id.*

126. Carpenter v. United States, 138 S. Ct. 2206 (2018).

127. *Id.* at 2218.

casually collected by wireless carriers today."[128] However, the Court stressed that its decision was narrow: "We do not disturb the application of *Smith* and *Miller* or call into question conventional surveillance techniques and tools, such as security cameras. Nor do we address other business records that might incidentally reveal location information."[129] Accordingly, it remains to be seen whether *Carpenter's* holding will be extended to other categories of personal information disclosed to third parties; until then, information picked up or shared with an IoT device presumptively falls beyond Fourth Amendment protections with regard to *ex post facto* police investigations.

IV. A NEW FRAMEWORK FOR PROTECTING PRIVACY INTERESTS

In light of long-standing jurisprudential norms underlying the development of privacy rights in the U.S., the current legal and constitutional standards fail to adequately protect individual privacy interests implicated by the collection of IoT data. So far, I have discussed privacy at length, but have not actually defined it—this is not because of some "big reveal" at the end of the note, but rather because the idea of privacy cannot be adequately captured in one definition, and I have admittedly used it in several different contexts throughout the course of this note. Neil Richards writes: "In recent years, many scholars have settled on an understanding of privacy as an umbrella term that encompasses a variety of related meanings."[130] Privacy is used to refer to property interests—the protection of the sanctity of one's home and possessions from unwanted intrusions. More broadly, privacy can refer to an individual's autonomy over their own bodies, relational and political associations, sexual orientations, confidences, thoughts, secrets, beliefs—all values we intuitively and instinctively hold sacred from unwanted disclosure to the public. Richards argues that we innately value *intellectual* privacy, or "the protection from surveillance or unwanted interference by others when we are engaged in the process of generating ideas and forming beliefs—when we're thinking reading, and speaking with confidants before our ideas are ready for public consumption."[131]

In any case, while it may be difficult to define, one fundamental aspect of privacy is that "it has a basic and intuitive feel to it."[132] For example, we are naturally inclined to view something like hacking into a baby monitor

128. *Id.* at 2219.
129. *Id.* at 2220.
130. NEIL M. RICHARDS, INTELLECTUAL PRIVACY: RETHINKING CIVIL LIBERTIES IN THE DIGITAL AGE 9 (2015) [hereinafter RICHARDS, INTELLECTUAL PRIVACY].
131. *Id.* at 95.
132. ALEXANDRA RENGEL, PRIVACY IN THE 21ST CENTURY 9 (2013).

and yelling profanities at an infant as a gross invasion of privacy,[133] as well as a constantly-listening SmartTV™ transferring the contents of every conversation in its immediate vicinity to some unidentified third party data processor for less-than-clear purposes.[134] We are equally likely to abhor the idea of an employer, unbeknownst to an employee, using their personal FitBit™ data to discover the employee was pregnant and subsequently firing them under some pretextual rationale. While the conceptions of privacy between these three examples vary—reflecting privacy of intimate spaces, conversations, and personal health information respectively—we intuitively value them and believe they should be protected.

I would argue that we should view the government's ability to access stored IoT data with impunity during criminal investigations as an equally grave invasion of individual privacy interests. As explained in Part III.A, the Stored Communications Act provides that the disclosure of electronically-stored information may be compelled by administrative subpoena, which requires that the investigators demonstrate a showing of mere 'relevance' to an ongoing investigation. And as the Bates case demonstrates, even if the data was collected without knowledge or consent (e.g. by a pre-installed smart utility meter), it is still discoverable and admissible at trial. Furthermore, even if that data is inherently unreliable (like the FitBit™ in the Risley case), or can be aggregated to reveal far more about an individual than one would reasonably assume possible (as Sotomayor points out about the GPS tracker data in *Jones*), neither the Federal Rules of Evidence nor the U.S. Constitution provide an adequate shield against the admissibility of that data. In fact, since the Third-Party Doctrine is still good law, the official stance of the Supreme Court on this issue is that we *cannot* have a reasonable expectation of privacy in information shared and processed by IoT manufacturers—even, presumably, information we had no idea we were disclosing in the first place.[135]

A great deal of literature has already been written about the Third-Party Doctrine and the various problems associated with its application to modern technologies,[136] and it may indeed face a major shake-up in the aftermath of the *Carpenter* decision.[137] Accordingly, I will not belabor the various doctrinal and philosophical qualms here. However, even if legal or

133. *See id.* at 13.
134. *See id.* at 12.
135. Ferguson, *supra* note 124, at 840.
136. *Id.* at 831–832 fn. 165.
137. Carpenter v. United States, 138 S. Ct. 2206 (2018).

regulatory changes are made concerning the government's *access* to IoT data in coming years, the problem of *surveillance* via IoT devices remains an unresolved and ever-present issue in the IoT sphere.[138]

In other words, the government may request ESI from an entity after the fact, or alternatively, it could actively monitor the user's behavior by simultaneously intercepting data transmitted by any number of IoT devices.[139] The emphasis here is on the latter of the two possibilities; even if the standards surrounding the acquisition of ESI for prosecutorial purposes are heightened, the current standards for the interception of IoT data, as it is simultaneously being communicated with its intended destination (namely the device's data processer), remain ill-equipped to protect individual privacy interests. The *Katz* reasonable expectation standard is outdated and cannot adequately respond to the various ways in which IoT products will inevitably be used in criminal investigations in coming years. Furthermore, the Trespass Doctrine has a very limited applicability, and is largely irrelevant in the era of sophisticated and ubiquitous wireless transmission of data.[140]

The reasonable expectation standard necessarily relies on societal expectations, but our societal expectations are shifting in ways that run contrary to the privacy interests we value, largely in part due to the pervasiveness and intrusiveness of IoT devices in our daily lives. Where we would have once been appalled by the idea of a speaker that was constantly listening to our conversations, even if it was only listening for a particular word or phrase, the Echo Dot™ was the most popular product in the 2017 holiday season on the world's largest online retailer's website.[141] In light of the Samsung SmartTV™ controversy, one commenter astutely notes: "Depressingly enough, all of this is just more evidence that 'yes, if

138. To clarify, surveillance by malicious actors via IoT devices is a distinct threat in and of itself, as discussed in Part IIC. That threat concerns the broad realm of cybersecurity and inadequate protections within individual IoT devices and their respective networks. The threat of surveillance as discussed here concerns the government using consumer IoT products for surveillance-oriented purposes during active investigations.

139. Former Director of National Intelligence James Clapper stated: "In the future, intelligence services might use the [internet of things] for identification, surveillance, monitoring, location tracking, and targeting for recruitment, or to gain access to networks or user credentials." Spencer Ackerman & Sam Thielman, *US Intelligence Chief: We Might Use the Internet of Things to Spy on You*, GUARDIAN (Feb. 9, 2016), https://www.theguardian.com/technology/2016/feb/09/internet-of-things-smart-home-devices-government-surveillance-james-clapper.; Former CIA Director David Petraeus stated: "[IoT] items of interest will be located, monitored, and remotely controlled through technologies such as radio-frequency identification, sensor networks, tiny embedded servers, and energy harvesters—all connected to the next-generation internet using abundant, low-cost, and high-power computing . . . [household spy devices] change our notions of secrecy [and prompt a rethink] of our notions of identity and secrecy." Spencer Ackerman, *CIA Chief: We'll Spy on You Through Your Dishwasher*, WIRED (Mar. 15, 2015, 5:35 PM), https://www.wired.com/2012/03/petraeus-tv-remote/.

140. Ferguson, *supra* note 124, at 838.

141. *See* Wong, *supra* note 43.

your smart gadget is connected to the internet, then it's probably collecting data on you.' So Samsung's privacy admission suddenly turns from surprise to status quo."[142] We keep our smart phones with us at all times, constantly transmitting our location data to our service providers.

In addition to the information we willfully (or inadvertently) disclose to third party vendors, we are now cognizant of the realities of dragnet NSA surveillance.[143] Where it was once a common, yet lighthearted joke across online message boards and social media platforms to say that someone was "on a list" after making a questionable or inflammatory comment, a Pew Research Center poll from 2015 found that 65% of Americans believe that there are not adequate limits on "what telephone and internet data the government can collect. . . . The majority view that there are not sufficient limits on what data the government gathers is consistent across all demographic groups."[144]

In sum, we value privacy and intimacy within our homes and amongst our relationships, yet we are becoming more and more accepting of intrusive IoT devices in our daily lives while simultaneously becoming more aware of and accepting of the fact that the government can (and does) have a nearly unlimited ability to intercept the data our IoT devices transmit. If our expectation of privacy is constantly and rapidly diminishing, how can we continue to apply the *Katz* reasonable expectation standard and rely on it to hold any weight? If we bring IoT devices into our private spaces, aware of their capacity for third party and governmental surveillance, how can we continue to reasonably expect privacy in conversations taking place in the vicinity of these devices?

Concededly, these concerns are tempered somewhat by Supreme Court decisions extending Fourth Amendment protections to other sophisticated surveillance techniques. Perhaps most relevant to the IoT context is *Kyllo v. United States*,[145] in which the Court held that the use of a high-tech thermal imaging device to scan a suspect's home for the presence of high-intensity lamps (used for indoor marijuana growth) constituted a search within the meaning of the Fourth Amendment. Writing for the majority, Justice Scalia stated: "Where, as here the Government uses a device that is not in general public use, to explore details of the home that would previously have been unknowable without

142. Orf, *supra* note 54.

143. *See generally NSA Spying*, ELECTRONIC FRONTIER FOUNDATION, https://www.eff.org/nsa-spying.

144. Mary Madden & Lee Rainie, *Americans' Attitudes About Privacy, Security and Surveillance*, PEW RESEARCH CENTER (May 20, 2015), http://www.pewinternet.org/2015/05/20/americans-attitudes-about-privacy-security-and-surveillance/.

145. Kyllo v. United States, 533 U.S. 27 (2001).

physical intrusion, the surveillance is a 'search' and is presumptively unreasonable *without* a warrant."[146] Scalia further reiterated: "We have said that the Fourth Amendment draws 'a firm line at the entrance to the house.'"[147] One could make an argument that surveillance via IoT devices is comparable to the thermal imaging device at issue in *Kyllo*—such a practice would reveal "details of the home" that were otherwise unknowable without physical intrusion, thus mandating a warrant.

While Scalia suggested the presence of a bright-line rule protecting the interior of the home, his opinion in *Kyllo* (and the precedent cited therein) relied on the *Katz* standard in reaching its conclusion: "[I]n the case of the search of the interior of homes—the prototypical and hence most commonly litigated area of protected privacy—there is a ready criterion, with roots deep in the common law, of the minimal expectation of privacy that *exists*, and that is acknowledged to be *reasonable*."[148] But what happens if this "minimal expectation of privacy" erodes entirely? What if we collectively decide that privacy, as we once knew it, is dead?[149] So long as Fourth Amendment protection is conditioned on an expectation of privacy—and a societal acknowledgment that the expectation is reasonable—Scalia's suggestion that a bright-line rule exists is fundamentally premature.

To reconcile this issue, I suggest we return to our roots. In 1890, Samuel Warren and Louis Brandeis co-authored *The Right to Privacy*,[150] one of the most influential articles on privacy rights in U.S. history and a guiding force behind the development of the four privacy torts in Prosser's *Restatements*.[151] Concerned about the increasingly invasive and offensive "gossip" industry in the press, the two scholars advocated for the development of codified privacy tort laws.[152] The article suggested that individuals have "a general right . . . to be let alone,"[153] while asserting

146. *Id.* at 40 (emphasis added).

147. *Id.* (citing Payton v. New York, 445 U.S. 573 (1980)).

148. *Id.* at 34.

149. Christopher Mims, *Privacy is Dead. Here's What Comes Next*, WALL ST. J., (May 6, 2018), https://www.wsj.com/articles/privacy-is-dead-heres-what-comes-next-1525608001; Agence France-Presse, *Privacy is Dead, Invasive Technology is Here to Stay*, INDUSTRYWEEK (Jan. 22, 2015), https://www.industryweek.com/technology/privacy-dead-invasive-technology-here-stay; Jacob Morgan, *Privacy Is Completely And Utterly Dead, and We Killed It*, FORBES (Aug. 19, 2014), https://www.forbes.com/sites/jacobmorgan/2014/08/19/privacy-is-completely-and-utterly-dead-and-we-killed-it/#61176bf031a7.

150. Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193 (1890).

151. Neil M. Richards & Daniel J. Solove, *Prosser's Privacy Law: A Mixed Legacy*, 98 CAL. L. REV. 1887, 1888 (2010) ("Whereas Warren and Brandeis planted the germinal seed for tort privacy, Prosser systematized and organized the law, giving it an order and legitimacy that it had previously lacked.").

152. Warren & Brandeis, *supra* note 150.

153. *Id.*

that preexisting property rights protect both tangible and intangible interests—interests encompassed by the nebulous term "[one's] inviolate personality."[154] The article also identified the framework for the privacy theory known broadly as Information Privacy:[155] "The common law secures to each individual the right of determining, ordinarily, to what extent his thoughts, sentiments, and emotions shall be communicated to others."[156] Rather than view privacy as an emotional or theoretical ideal, they viewed it as an actual and innate right to choose when, how, and to whom one disclosed their personal information.

While Warren and Brandeis' article had a noticeable impact in the development of U.S. privacy rights, their conceptualization of privacy as autonomy over the disclosure of personal information was far from novel. The idea of privacy as an individual property right, and more fundamentally, the idea of property as a secure, controllable interest of a sole individual, has roots reaching as far back Aristotle's writings.[157] Aristotle identifies four conditions that must be met to qualify fully as being 'wealthy,' (1) and (2) speak not just to wealth, but ownership in general; (3) maintains that one's properties must be secure; and (4) Maintains that one's properties are one's own.[158] As translated by Miller, "A criterion of 'security' is possession in a given place and in such a manner that the use of the objects is up to oneself; and a criterion of 'being one's own or not' is when the alienation of it is up to oneself."[159] If we view property as the fundamental right to security and alienability of our possessions, and if we consider privacy as a kind of possessory interest in our personal information as Warren and Brandeis suggest, their conclusion that privacy is more accurately understood as a property interest stands on firm logical and philosophical grounds.

I would advocate for a return to this line of thinking as privacy law continues to fluctuate in our increasingly interconnected, IoT-enabled world. We should not be asking what *society* reasonably expects to be private, as social norms are changing as rapidly as our new technologies are developing. Instead, when we analyze whether a search occurs under the Fourth Amendment such that a warrant is necessary, we should focus on the individual and how they choose to disclose (or not disclose) their personal information. In other words, only if an individual *knowingly* and

154. *Id.*
155. *See generally* RICHARDS, INTELLECTUAL PRIVACY, *supra* note 130.
156. Warren & Brandeis, *supra* note 150.
157. Fred D. Miller, Jr., *Aristotle on Property Rights*, *in* ESSAYS IN ANCIENT GREEK PHILOSOPHY IV: ARISTOTLE'S ETHICS 229 (John Peter Anton et al. eds., 1991).
158. *Id.*
159. *Id.*

voluntarily discloses information with an IoT device, and only if they are cognizant of the kinds of inferences that can be made from that data, should that information fall beyond the constitutional safeguard of the Fourth Amendment warrant requirement. To be clear, I am not the first to advocate for a shift towards an information privacy-oriented scheme,[160] nor do I offer much in terms of specific suggestions to effectuate such a scheme—I am simply arguing here that the proliferation of IoT devices makes the necessity of reconceptualizing existing privacy standards all that more urgent. If we view privacy rights in this way as control over one's information, rather than what a judge believes society would expect to be private, we can eliminate the risk of new technologies shifting our social norms in ways that conflict with the privacy values we instinctively and naturally wish to protect.

---

160. *See generally* David Alan Sklansky, *Too Much Information: How Not to Think About Privacy and the Fourth Amendment*, 102 CAL. L. REV. 5 (2014); Neil M. Richards, *The Dangers of Surveillance*, 126 HARV. L. REV. (2013); Paul Schwartz, *Privacy and Democracy in Cyberspace*, 52 VAND. L. REV. (1999).