SMART DEVICES WON'T BE "SMART" UNTIL SOCIETY DEMANDS AN EXPECTATION OF PRIVACY

*Katherine E. Tapp**

I. INTRODUCTION

On March 10, 2015, police were called to a home in Lancaster, Pennsylvania where a woman, Jeannine M. Risley, 44, reported that a man in his thirties had come into the home while she was asleep and violently raped her.[1] Risley gave a brutal account of her assault and described the man with vivid detail.[2] During the investigation, Risley allowed police to access the data on her Fitbit which had been found on the floor near the alleged attack.[3] Per the affidavit:

> The information collected from the fit bit [sic] device showed that Nina was awake and walking around the entire night prior to the incident and did not go to bed as reported. The Fitbit shows activity up until the time of the call and then again only when it is collected by your Affiant. That based on the above and additional evidence your Affiant believes that the Defendant Nina Risley was not raped as reported and fabricated the entire incident.[4]

There was also no evidence of footprints leading to the home, despite the yard being covered in snow.[5] The findings led a judge to order Risley to complete two years of probation and 100 hours of community service for

---

* J.D. Candidate, May 2018, Louis D. Brandeis School of Law, University of Louisville; B.A., May 2009, Morehead State University. I am grateful to my husband, Joe, for his patience and support, and to my dad for his constant encouragement. I would also like to thank Professor Abramson for his guidance and instruction. Finally, thanks to the editors of the University of Louisville Law Review for their hard work while editing this Note. Any remaining errors are my own.

[1] Affidavit of Probable Cause ¶ 1, Commonwealth v. Risley, CP-36-CR-0002937-2015 (Pa. Ct. C.P. Apr. 17, 2015) [hereinafter Risely Affidavit], http://online.wsj.com/public/resources/documents/2016_0421_PAvRisley.pdf (order appended); Jacob Gershman, *Prosecutors Say Fitbit Device Exposed Fibbing in Rape Case*, WALL ST. J.: L. BLOG (Apr. 21, 2016, 1:53 PM), http://blogs.wsj.com/law/2016/04/21/prosecutors-say-fitbit-device-exposed-fibbing-in-rape-case.

[2] Risley Affidavit, *supra* note 1, ¶ 2.

[3] Gershman, *supra* note 1 (citing Risely Affidavit, *supra* note 1).

[4] Risely Affidavit, *supra* note 1, ¶¶ 9–10.

[5] *Id.* ¶ 3.

reporting a false alarm, tampering with physical evidence, and making a false report.[6]

As the technology behind wearable devices expands and diversifies, cases like Risley's may become more common.[7] According to a recent study by CCS Insight, an industry analyst firm, the wearables market is set to increase threefold over the next five years; by 2019, an estimated $25 billion worth of wearable devices will be sold.[8] For purposes of litigation, privacy concerns arising from the data collected by wearables may justify a distinction between medical gadgets prescribed by health care providers and mainstream devices available in the consumer sector. What is the relationship between the law and the data produced by different categories of personal smart devices? Each group may have different privacy expectations.

Several FDA-approved wearable devices are already prescribed for patient use: insulin monitors, cardiac event monitors, smart-thermometers, electronic diaries for clinical trials, smart-inhalers for people with asthma, and more.[9] Proponents argue these tools empower individuals to take control of their health while providing physicians with a more complete and accurate picture of their patients' wellbeing.[10]

But this healthcare potential is offset by data privacy and security challenges.[11] Health data is more vulnerable than other types of data; it can't be replaced like a credit card, and there are no good remedies when a person's medical records are improperly accessed.[12] Wearable technology is highly sophisticated and can monitor and share user activity with a variety of applications and devices.[13] "These tools are capable of measuring brain activity, calorie intake, miles walked and run, swimming strokes, blood oxygen and blood sugar levels, and heart rates. They are both fitness coach

---

[6] *See* Order, *Risley*, CP-36-CR-0002937-2015, http://online.wsj.com/public/resources/documents/2016_0421_PAvRisley.pdf (affidavit appended).

[7] Wearable devices are starting to impact civil litigation as well. In 2014, McLeod Law, a firm in Calgary, Canada, worked the first known personal injury case that used activity data from a Fitbit to help show their client's injuries from a car accident. *See* Parmy Olson, *Fitbit Data Now Being Used in the Courtroom*, FORBES (Nov. 16, 2014, 4:19 PM), http://www.forbes.com/sites/parmyolson/2014/11/16/fitbit-data-court-room-personal-injury-claim/#5185029e209f.

[8] Press Release, CCS Insight, Wearables Market to be Worth $25 Billion by 2019 (Aug. 2015), http://www.ccsinsight.com/press/company-news/2332-wearables-market-to-be-worth-25-billion-by-2019-reveals-ccs-insight.

[9] Brian Dolan, *23 Notable FDA Clearances for Digital Health Apps, Devices So Far This Year*, MOBIHEALTHNEWS (Sept. 24, 2014), http://www.mobihealthnews.com/36795/23-notable-fda-clearances-for-digital-health-apps-devices-so-far-this-year.

[10] Sarah Kellogg, *Every Breath You Take: Data Privacy and Your Wearable Fitness Device*, 72 J. MO. B. 76, 76 (2016).

[11] *Id.*

[12] *Id.*

[13] *Id.*

and a proverbial 'black box' for a consumer's health."[14] Because unsuspecting users are unaware of how data from these devices is used and shared, consumers appear willing to sacrifice privacy for the benefits associated with these devices.[15]

Societal expectations of privacy determine when both Fourth and Fifth Amendment protections apply.[16] The framework for evaluating those expectations is whether the area being searched or the item being seized "falls within a protected zone of privacy."[17] If no such expectation of privacy exists, "then no exception to the warrant requirement is needed to search the area."[18] Courts will soon be faced with the challenge of deciding which zone the information from wearables and other personal smart devices falls into.

The purpose of this Note is to consider what impact wearable technology (and other types of digital data) will have on traditional privacy law. Part II will examine the dawn of "industry 4.0," emphasizing the recent advances in information technologies that have fueled the proliferation of personal smart devices. Part III will analyze 1) the possible Fourth Amendment protections available when law enforcement wishes to access an individual's digital data, and 2) the potential applications of Fifth Amendment immunity for the production of digital data. In addition, Part III considers the difficulties of interpreting user-created data from an evidentiary standpoint by focusing on the Sixth Amendment, hearsay, and reliability.

Part IV is a policy recommendation that advocates for the grouping of all digital data derived from personal smart devices (wearables, medical wearables, smart phones, smart speakers, home automation devices, etc.) into one category, deserving of the highest privacy expectations when applying

---

[14] *Id.*

[15] *See* Melissa W. Bailey, Note, *Seduction by Technology: Why Consumers Opt Out of Privacy by Buying into the Internet of Things*, 94 TEX. L. REV. 1023, 1024–25 (2016); Press Release, ISACA, ISACA Survey: Most Consumers Aware of Major Data Breaches but Fewer Than Half Have Changed Key Shopping Behaviors (Nov. 2014), https://www.isaca.org/About-ISACA/Press-room/News-Releases/2014/Pages/ISACA-Survey-Most-Consumers-Aware-of-Major-Data-Breaches-but-Fewer-than-Half-Have-Changed-Shopping-Behavior.aspx.

[16] *See* United States v. Katz, 389 U.S. 347, 360 (1967) (Harlan, J., concurring) (explaining that a person must first have an actual, subjective expectation of privacy, and second, the expectation must be one society recognizes as reasonable). Likewise, Fifth Amendment immunity against the compelled production of documents applies "only if the individual resisting production had a reasonable expectation of privacy with respect to the evidence." Fisher v. United States, 425 U.S. 391, 424 (1976) (citing Couch v. United States, 409 U.S. 322, 328, 336 (1973)); *see also* Thomas J. Koffer, Note, *All Quiet on the Paper Front: Asserting A Fifth Amendment Privilege to Avoid Production of Corporate Documents in* in Re Three Grand Jury Subpoenas Duces Tecum Dated January 29, 1999, 46 VILL. L. REV. 547, 578 (2001).

[17] United States v. Miller, 425 U.S. 435, 440 (1976) (citing Hoffa v. United States, 385 U.S. 293 (1966)).

[18] 24 ROBERT RAMSEY, NEW JERSEY PRACTICE SERIES, MOTOR VEHICLE LAW AND PRACTICE § 4:40 (4th ed. 2016).

constitutional protections. This section includes a model statute that addresses the privacy concerns that arise when law enforcement wish to access digital data from personal smart devices.

II. HISTORY – THE RISE OF PERSONAL SMART DEVICES

Recent advances in information technologies have happened at an unprecedented rate, revolutionizing how people create, share, and store digital data.[19] This section examines how developments in automation, artificial intelligence, and the Internet of Things have ushered in what some are calling "the fourth industrial revolution" in hopes of better understanding what—if any—categories should be used to classify our expectation of privacy from various digital data sources.[20]

The fourth industrial revolution, or "industry 4.0," represents the union of recent advances in "artificial intelligence, 3-D printing, robotics, Big Data and data science, genetics, medical imaging, and computer vision."[21] Industry 4.0 blurs the lines between the "physical, digital and biological" to create machines that can think, self-replicate, and share information.[22] These advancements have combined in ways that are revolutionizing professions and industries across the globe.[23]

Three tech trends in particular highlight how industry 4.0 is transforming daily lives and threatening traditional privacy protections in the process. The first, advanced automation, has been characterized as the "rise of the robots."[24] Competitive pressure to reduce assembly time, create faster setup, experience fewer errors, and improve quality has led to machines that combine different functions instead of the single-function tools traditionally used in manufacturing.[25] What formerly required human operation or monitoring is being systematically replaced by computer controllers,

---

[19] Mark Barrenechea, *The Tech Trends Set to Dominate the Digital Revolution*, IT PROPORTAL (Feb. 1, 2017), http://www.itproportal.com/features/the-tech-trends-set-to-dominate-the-digital-revolution.

[20] *Id.*

[21] *March of the Machines: The Fourth Industrial Revolution*, CYBER SECURITY INTELLIGENCE (May 26, 2016), https://www.cybersecurityintelligence.com/blog/march-of-the-machines-1330.html; *see also* Bernard Marr, *Why Everyone Must Get Ready for the 4th Industrial Revolution*, FORBES (Apr. 5, 2016), http://www.forbes.com/sites/bernardmarr/2016/04/05/why-everyone-must-get-ready-for-4th-industrial-revolution/#44b67bc879c9.

[22] Marr, *supra* note 21.

[23] *See id.*

[24] *See* Simon Worrall, *Will the Rise of the Robots Implode the World Economy?*, NAT'L. GEOGRAPHIC (June 3, 2015), http://news.nationalgeographic.com/2015/06/150603-science-technology-robots-economics-unemployment-automation-ngbooktalk.

[25] Jonathan Hujsak, *The Fourth Industrial Revolution: Factors of Production Misalignment on a Global Scale*, J. OF COST MGMT., Sept./Oct. 2016, 2016 WL 4705792.

allowing for "high-speed, personalized manufacturing that produces products as needed (i.e., minimal or no inventory)," and enabling each product to be customized "from hundreds or thousands of possibilities."[26]

The rise of the robots is not limited to manufacturing. E-commerce giant Amazon has been utilizing advanced automation for years, applying the robotics principles that improved manufacturing efficiency to logistics and material-handling fields.[27] Back in 2012, Amazon purchased a robotic outfit company for a staggering $750 million, then followed up by introducing some 30,000 robots to its warehouse operations.[28] In early 2016, Wal-Mart announced it would cut 7,000 jobs in lieu of new automation capabilities, and other retail companies like Foxconn and Wendy's made similar headlines (60,000 jobs lost in Foxconn's case).[29] These announcements portend a future in line with findings from a 2016 survey by the World Economic Forum predicting developments in genetics, artificial intelligence ("A.I."), and robotics could result in the loss of over five million jobs by 2020.[30]

Advances in automation have not occurred in a bubble, instead sharing a complicated relationship with advances in the other two technological trends discussed here: artificial intelligence and the Internet of Things. Each sphere of growth is interrelated, complicating the categorization of our expectations of privacy.

The second tech trend responsible for transforming disciplines across the board is artificial intelligence.[31] By relegating "mundane" decisions to machines, A.I. enables organizations to expand in previously unimagined ways.[32] A.I. can serve not only as a labor-replacing mechanism, but as a "mind-expanding strategy."[33] In retail, for example, A.I. is increasingly being

---

[26] *Id.*

[27] *Id.*

[28] *Id.*

[29] LuLu Chang, *WalMart Is Cutting 7,000 Jobs Due to Automation, and It's Not Alone*, DIGITAL TRENDS (Sept. 2, 2016), http://www.digitaltrends.com/business/walmart-cuts-jobs-for-robots.

[30] Marcia Breen, *Your Job Might Be One of 5 Million Replaced by Robots by 2020*, NBC NEWS: TECH NEWS (Jan. 20, 2016, 3:39 AM), http://www.nbcnews.com/tech/tech-news/robot-may-take-your-job-next-few-years-n499556.

[31] *See* Kevin Maney, *How Artificial Intelligence and Robots Will Radically Transform the Economy*, NEWSWEEK (Nov. 30, 2016, 8:10 AM), http://www.newsweek.com/2016/12/09/robot-economy-artificial-intelligence-jobs-happy-ending-526467.html.

[32] Joe McKendrick, *Artificial Intelligence Doesn't Just Cut Costs, It Expands Business Brainpower*, FORBES (Jan. 24, 2017, 12:03 PM), http://www.forbes.com/sites/joemckendrick/2017/01/24/artificial-intelligence-doesnt-just-cut-costs-it-expands-business-brainpower/#29f82f4b39f8.

[33] *Id.*

used to power insights that "formerly would have only emerged from human intuition."[34]

Artificial intelligence is no longer a sci-fi concept out of a Ridley Scott movie. Millions of Americans rely on A.I. systems like Alexa, Siri, Cortana, and Google Assistant to streamline their daily lives.[35] These digital assistants respond to ordinary language and can anticipate users' needs.[36] "Whether providing direct answers to spoken questions, sending warnings when traffic problems might make you late for a meeting or automatically putting appointments in your calendar, the aim is the same: to make digital existence less of a chore."[37]

Digital assistants like Amazon's Alexa work by gathering immense amounts of information about users: patterns and data from e-mail, search queries, online purchases, social media activity, GPS tracking, and more.[38] Using complicated algorithms that mimic the neural network of the human brain, these A.I. personalities can learn from the millions of requests they receive from users all over the world.[39] Each request gets tagged with a unique device ID and stored with the corresponding company to be mined for information at the corporation's leisure.[40] Amazon and other companies that store the data on their own servers insist that the information is used to improve their products.[41] But it is alarming that users have no say in this decision, especially considering that the economic potential for companies to

---

[34] Rachel Arthur, *Future of Retail: Artificial Intelligence and Virtual Reality Have Big Roles to Play*, FORBES (June 15, 2016, 2:15 PM), http://www.forbes.com/sites/rachelarthur/2016/06/15/future-of-retail-artificial-intelligence-and-virtual-reality-have-big-roles-to-play/#7c74f85e420c.

[35] John Koetsier, *Alexa, Google, Siri, Cortana: 24.5M Voice-First Devices Will Ship This Year*, FORBES (Jan. 26, 2017, 1:22 PM), http://www.forbes.com/sites/johnkoetsier/2017/01/26/alexa-google-siri-cortana-24-5m-voice-first-devices-will-ship-this-year/#527044ae28d7.

[36] Richard Waters, *Siri, Alexa, Cortana and the Unstoppable Rise of the Digital Assistant*, FIN. REV. (Sept. 25, 2016, 1:42 PM), http://www.afr.com/technology/apps/business/siri-alexa-cortana-and-the-unstoppable-rise-of-the-digital-assistant-20160925-grnxvj.

[37] *Id.*

[38] Nash David, *Siri, Google Now and Cortana: How Digital Assistants Predict What You Need*, FIRSTPOST (Sept. 21, 2015, 10:22 AM), http://tech.firstpost.com/news-analysis/siri-google-now-and-cortana-how-digital-assistants-predict-what-you-need-281997.html.

[39] Leonard Klie, *Neural Networks Reach into Virtual Assistants*, CRM MAG. (Sept. 2014), http://www.destinationcrm.com/Articles/Columns-Departments/Insight/Neural-Networks-Reach-into-Virtual-Assistants-98749.aspx; David, *supra* note 38.

[40] Kaveh Waddell, *The Privacy Problems with Digital Assistants*, ATLANTIC (May 24, 2016), https://www.theatlantic.com/technology/archive/2016/05/the-privacy-problem-with-digital-assistants/483950.

[41] Sharon Profis, *Amazon Echo Saves All Your Voice Data. Here's How to Delete It*, C-NET (Jan. 22, 2015, 12:35 PM), https://www.cnet.com/how-to/amazon-echo-saves-all-your-voice-data-heres-how-to-delete-them.

exploit this information (by selling it to third parties for precisely-targeted advertising) has been estimated at between $500 million and $1 billion.[42]

Artificial intelligence is closely associated with the final tech trend emphasized by this Note: the Internet of Things ("IoT"), a term defined by the Federal Trade Commission as an "interconnected environment where all manner of objects have a digital presence and the ability to communicate with other objects and people."[43] In short, the IoT embraces a reality where devices ranging from cell phones to wearables to our washing machines all connect to the internet and to one another, building a huge, widely-varying network of connectivity.[44] Imagine a "digital nervous system" that incorporates advanced automation and artificial intelligence to create a "hyper-connected environment [that] will monitor, measure, and automate tasks."[45]

To truly understand the scope of the IoT, consider that every second, 127 devices are added to the internet.[46] By 2020, tech forecasters predict that over 50 billion connected devices will be in use and that "the total volume of data generated by IoT will reach 600 ZB per year . . . 275 times higher than projected traffic going from data centers to end users/devices (2.2 ZB); 39 times higher than total projected data center traffic (15.3 ZB)."[47] Economically, the IoT will contribute between $4 trillion and $11 trillion per year globally by 2025.[48]

In many respects, industry 4.0 is making life simpler, easier and more fun. Concepts of "open enterprise" allow companies to "offer themselves through other apps, websites, and device functions . . . so you can order an

---

[42] Marcus Wohlsen, *Amazon's Next Big Business is Selling You*, WIRED (Oct. 16, 2012, 11:00 AM), https://www.wired.com/2012/10/amazon-next-advertising-giant.

[43] FED. TRADE COMM'N, INTERNET OF THINGS: PRIVACY & SECURITY IN A CONNECTED WORLD 1 (Jan. 2015), https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf.

[44] *See* Jacob Morgan, *A Simple Explanation of 'The Internet of Things'*, FORBES (May 13, 2014, 12:05 AM), https://www.forbes.com/sites/jacobmorgan/2014/05/13/simple-explanation-internet-things-that-anyone-can-understand/#7def02111d09.

[45] *How Much Data Will the Internet of Things (IoT) Generate by 2020?*, PLANET TECH. (Oct. 13, 2016), https://planetechusa.com/blog/how-much-data-will-the-internet-of-things-iot-generate-by-2020.

[46] David Evans, *Introducing the Wireless Cow*, POLITICO (June 29, 2015, 5:25 AM), http://www.politico.com/agenda/story/2015/06/internet-of-things-growth-challenges-000098.

[47] Joe McKendrick, *With Internet of Things and Big Data, 92% of Everything We Do Will Be in the Cloud*, FORBES (Nov. 13, 2016, 1:02 PM), http://www.forbes.com/sites/joemckendrick/2016/11/13/with-internet-of-things-and-big-data-92-of-everything-we-do-will-be-in-the-cloud/#6227b16b593f; Matthew Murray, *Moving Toward a World of 50 Billion Connected Devices*, PC MAG. (Aug. 17, 2016, 3:30 PM), http://www.pcmag.com/news/347086/moving-toward-a-world-of-50-billion-connected-devices.

[48] James Manyika et al., *Unlocking the Potential of the Internet of Things*, MCKINSEY GLOBAL INST. (June 2015), http://www.mckinsey.com/businessfunctions/business-technology/our-insights/the-internet-of-things-the-value-of-digitizing-the-physical-world.

Uber directly through Google."[49] Augmented and virtual reality burst on the scene in 2016 with the release of Facebook's Oculus Rift and over 100 million downloads of the augmented reality app, Pokémon Go.[50] In December 2016, Amazon opened the first checkout-free grocery store, where shoppers walk in, grab what they want, and walk out; their orders post to their Amazon accounts.[51] Whether contemplating wearables like Fitbit or home automation devices like Amazon Echo, the reality of privacy in 2017 is that personal information is no longer kept in "desks [and] file cabinets" as contemplated by the Framers.[52] Rather, Americans travel with it constantly, never further away than a quick glance at their newest gadgets. Moreover, the kinds of information being gathered is becoming more and more personal, with health information and predictive analytics creating detailed, and frequently intrusive, impressions of people's lives.[53]

III. ANALYSIS – EXPECTATION OF PRIVACY, THE FIFTH AMENDMENT, AND EVIDENTIARY CONSIDERATIONS

Having highlighted the recent advances in information technology that are fueling the proliferation of personal smart devices, how can traditional expectations of privacy be modernized to encompass the new, technological reality? This section emphasizes the weakness of arguments favoring differing expectations of privacy for cell phones, wearables, medical devices, and other gadgets that rely on automation, connectivity, and data-gathering. Part B examines Fifth Amendment immunity in the context of compelled production of data from personal smart devices, and Part C highlights the evidentiary difficulties inherent in gathering and presenting digital data.

---

[49] Jayson DeMers, *The Top 7 Technology Trends That Dominated 2016*, FORBES (Dec. 15, 2016), http://www.forbes.com/sites/jaysondemers/2016/12/15/the-top-7-technology-trends-that-dominated-2016/#d1586801ef08.

[50] *Id.*

[51] Davey Alba, *Only Amazon Could Make a Checkout Free Grocery Store a Reality*, WIRED (Dec. 06, 2016), https://www.wired.com/2016/12/amazon-go-grocery-store.

[52] *See* Christine S. Scott-Hayward et. al., *Does Privacy Require Secrecy? Societal Expectations of Privacy in the Digital Age*, 43 AM. J. CRIM. L. 19, 41 (2015).

[53] *See, e.g.*, Charles Duhigg, *How Companies Learn Your Secrets*, N.Y. TIMES: MAG. (Feb. 16, 2012), http://www.nytimes.com/2012/02/19/magazine/shopping-habits.html. Target used predictive analysis to "guess" which customers were pregnant, then disclosed that information to marketers without authorization. *Id.* The marketers mailed advertising material to homes—even to women who had not announced their pregnancies publicly.

A. Expectation of Privacy in the Digital Era

"[T]echnology has two razor-sharp edges. . . . [O]ne edge can be employed to preserve a nation's security, the other can imperil its very essence."[54] The tension between technology and privacy is perhaps most noticeable in conflicts arising between the government and the individual. The former has access to previously unimagined eavesdropping equipment, electronic tracking devices, and aerial surveillance.[55] While the goal of these advancements is to keep society safe from violence and disorder, they create barriers for people wishing to prevent the government from encroaching on their private activities.[56] "The Fourth Amendment is an acknowledgment by the Framers of our Constitution that liberty and social order are in tension with one another. It reflects their best effort to strike and capture the most desirable balance between those two goals."[57] Maintaining the balance between liberty and social order becomes increasingly difficult as traditional rationales of Fourth Amendment protections clash against previously unimagined technology. The Fourth Amendment provides:

> The right of the people to be secure in their persons, houses, papers, and effects, against *unreasonable* searches and seizures, shall not be violated and no Warrants shall issue, but upon *probable cause*, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.[58]

When law enforcement conducts a search to uncover evidence of criminal wrongdoing, Fourth Amendment case law presumes that reasonableness[59] generally requires a warrant.[60]

The Framers' intent about the scope of privacy is still informative, though the Framers could not have anticipated the ubiquity of technology in modern society. At common law and at the time of the Fourth Amendment's adoption, the latter's inclusion of particularity requirements for places searched and people seized reflected privacy concerns in preventing "fishing" expeditions (as the King's men were wont to do via their writs of

---

[54] James J. Tomkovicz, *Technology and the Threshold of the Fourth Amendment: A Tale of Two Futures*, 72 MISS. L.J. 317, 320 (2002).

[55] *Id.* at 320–21.

[56] *Id.* at 319–21.

[57] *Id.* at 324–25.

[58] U.S. CONST. amend. IV (emphasis added).

[59] *See* Brigham City v. Stuart, 547 U.S. 398, 403 (2006) (holding that reasonableness is the touchstone of the Fourth Amendment).

[60] Riley v. California, 134 S. Ct. 2473, 2482 (2014).

assistance).[61] The modern preference for pre-search or pre-seizure proof of probable cause reflects the Framers' belief that an impartial judge or magistrate can evaluate the need for a particular search or seizure.[62] Thus, warrantless searches are "per se unreasonable" and limited to well-established exceptions.[63]

Riley v. California considered one of those exceptions—a search incident to an arrest—when the defendant was stopped for a traffic violation that eventually led to his arrest on weapons charges.[64] An officer searching Riley seized and accessed a cell phone found on Riley's person.[65] In deciding whether the search should be barred by an expectation of privacy in our cell phone data, the Supreme Court considered "three related precedents [*Chimel*, *Robinson*, and *Gant*] set[ting] forth the rules governing . . . [when] officers may search property on or near the arrestee."[66] As the Court has acknowledged since 1914, "the right on the part of the government, always recognized under English and American law, to search the person of the accused when legally arrested to discover and seize the fruits or evidences of crime."[67]

Chimel v. California defined the scope of the search-incident-to-arrest exception to the warrant requirement.[68] Police arrested Chimel inside his home and then searched his entire house.[69] The Supreme Court created the following rule:

> When an arrest is made, it is reasonable for the arresting officer to search the person arrested in order to remove any weapons that the latter might seek to use in order to resist arrest or effect his escape. Otherwise, the officer's safety might well be endangered, and the arrest itself frustrated. In addition, it is entirely reasonable for the arresting officer to search for and seize any evidence on the arrestee's person in order to prevent its concealment or destruction.... There is ample justification, therefore, for a

---

[61] "[W]rits of assistance used in the Colonies noted only the object of the search—any uncustomed goods—leaving customs officials completely free to search any place where they believed such goods might be." Steagald v. United States, 451 U.S. 204, 220 (1981).

[62] *See* Thomas Y. Davies, *Recovering the Original Fourth Amendment*, 98 MICH. L. REV. 547, 576 (1999).

[63] United States v. Katz, 389 U.S. 347, 357 (1967) (majority opinion).

[64] *Riley*, 134 S. Ct. at 2477.

[65] *Id.* at 2480.

[66] *Id.* at 2483.

[67] *Id.* at 2482 (citing Weeks v. United States, 232 U.S. 383, 392 (1914)).

[68] Chimel v. California, 395 U.S. 752, 755–56 (1969); *see also* Tristan M. Ellis, Note, *Reading Riley Broadly: A Call for a Clear Rule Excluding All Warrantless Searches of Mobile Digital Devices Incident to Arrest*, 80 BROOK. L. REV. 463, 471 (2015).

[69] *Chimel*, 395 U.S. at 753–54.

> search of the arrestee's person and the area 'within his immediate control'—construing that phrase to mean the area from within which he might gain possession of a weapon or destructible evidence.[70]

The warrantless search of Chimel's home did not fit within the search-incident-to-arrest exception because, after serving Chimel with a valid arrest warrant for burglary, the police proceeded to conduct a warrantless search of the entire home, including the garage, attic, and a small workshop.[71] Absent sufficient exigent circumstances, such an invasion of privacy is not justified under the Fourth Amendment, even when police have reason to suspect the home contains evidence.[72] Although the police were able to locate numerous stolen items, the situation lacked the urgency necessary to justify not obtaining a warrant.[73]

Chimel described the search-incident-to-arrest exception as being severely limited in scope; namely, it is "reasonable for the arresting officer to search the person arrested in order to remove any weapons that the latter might seek to use in order to resist arrest or effect his escape," and it is "reasonable for the arresting officer to search for and seize any evidence on the arrestee's person in order to prevent its concealment or destruction."[74] However, the latter circumstance is limited to the "area into which an arrestee might reach in order to grab a weapon or evidentiary items."[75] This is significant because it creates precise rationales for seizing objects found on an arrestee's person.[76] Wearable and mobile smart technology inherently falls into this category. While it is unlikely a wearable could be used as a weapon, what about the destruction of evidence prong? As the Court noted in the next case, such perils are present in all custodial arrests.[77]

United States v. Robinson expanded *Chimel* by holding that the previously enumerated risks applied in *all* custodial arrests, regardless of the nature of the arrest and even without a direct threat to either the preservation of evidence or the officer's safety.[78] The Court upheld the search of a cigarette pack found on the defendant's person during the course of arrest.[79] Although custodial arrests are a "significant intrusion of state power into the

---

[70] *Id.* at 762–63.
[71] *Id.* at 753–54.
[72] *Id.* at 763.
[73] *Id.* at 754, 761.
[74] *Id.* at 763.
[75] *Id.*
[76] Ellis, *supra* note 68, at 471.
[77] United States v. Robinson, 414 U.S. 218, 235–36 (1973).
[78] Riley v. California, 134 S. Ct. 2473, 2484–85 (2014) (citing *Robinson*, 414 U.S. at 224).
[79] *Robinson*, 414 U.S. at 223.

privacy of one's person . . . if the arrest is lawful, the privacy interest guarded by the Fourth Amendment is subordinated to a legitimate and overriding governmental concern."[80] Thus, "no reason then exists to frustrate law enforcement by requiring some independent justification for a search incident to a lawful arrest."[81]

Arizona v. Gant involved a defendant who was arrested for driving on a suspended license; he was handcuffed and placed in a patrol car before officers searched his car and found cocaine.[82] The Court held that such searches, by the considerations laid out in *Chimel*, applied to the area within which an arrestee might destroy evidence or grab a weapon.[83] To limit this exception to vehicle searches where the arrestee was no longer in or near vehicle, the Court required proof that the arrestee's access to a weapon or contraband was a "reasonable possibility."[84]

Ultimately, the *Riley* Court "decline[d] to extend *Robinson's* categorical rule to searches of data stored in cell phones."[85] The Court relied on its traditional approach to creating an exception to the warrant requirement, noting that "absent more precise guidance from the founding era," the question of "whether to exempt a given type of search from the warrant requirement" will be decided by weighing "the degree to which it intrudes upon an individual's privacy" against "the degree to which it is needed for the promotion of legitimate governmental interests."[86] Unlike *Robinson*, "a search of digital information on a cell phone does not further the government interests [preservation of evidence and officer safety] identified in *Chimel*, and implicates substantially greater privacy interests than a brief physical search."[87]

Significantly, the *Riley* court discussed at length how cell phones differ from other objects that might be carried on an arrestee's person:

> Notably, modern cell phones have an immense storage capacity. Before cell phones, a search of a person was limited by physical realities and generally constituted only a narrow intrusion on privacy.

---

[80] *Id.* at 218.

[81] *Id.*

[82] Arizona v. Gant, 556 U.S. 332, 335 (2009).

[83] *Id.*

[84] *Id.* Recognizing the possibility for confusion between the outcome of *Gant* with another important search-incident-to-arrest case, *Thornton v. United States*, the Court tried to clarify that *Thornton* involved a drug-offense while Gant was arrested for driving on a suspended license; in the latter, there was no concern that evidence relating to the driving offense was located in Gant's vehicle. *Id.* at 344.

[85] Riley v. California, 134 S. Ct. 2473, 2478 (2014).

[86] *Id.* (citing Wyoming v. Houghton, 526 U.S. 295, 300 (1999)) (internal quotation marks omitted).

[87] *Id.* at 2478.

> But cell phones can store millions of pages of text, thousands of pictures, or hundreds of videos. This has several interrelated privacy consequences. First, a cell phone collects in one place many distinct types of information that reveal much more in combination than any isolated record. Second, the phone's capacity allows even just one type of information to convey far more than previously possible. Third, data on the phone can date back for years. In addition, an element of pervasiveness characterizes cell phones but not physical records. A decade ago officers might have occasionally stumbled across a highly personal item such as a diary, but today many of the more than 90% of American adults who own cell phones keep on their person a digital record of nearly every aspect of their lives.[88]

The scope of the privacy interests at stake is further complicated by the fact that the data viewed on many modern cell phones may in fact be stored on a remote server. Thus, a search may extend well beyond papers and effects in the physical proximity of an arrestee, a concern that prosecutors recognize but cannot definitively foreclose.[89]

The advent of industry 4.0 means that the qualities identified in *Riley* which distinguish cell phones from other types of objects normally found on an arrestee's person apply to *all personal smart devices*, whether worn on the wrist or sitting on a desk at home. Increasingly, wearables and other smart devices link with the user's phone, tablet, laptop, and other household gadgets, so that accessing one could potentially provide access to all the information and data gathered about a person by the myriad of smart devices proliferating modern daily life.[90] Moreover, companies encourage users to share their activity on Facebook and other social media platforms, forcing courts to engage in arbitrary line-drawing based on the user's privacy settings (e.g., whether a Facebook post was shared to "friends" or to the public).[91] Like the warrant requirement, expectations of privacy center on a reasonableness standard—a standard that is bound to evolve as advances in automation, A.I., and the IoT continue to influence modern society.[92]

---

[88] *Id.* at 2478–79.

[89] *Id.* at 2478–79.

[90] See generally Antigone Peyton, *A Litigator's Guide to the Internet of Things*, 22 RICH. J.L. & TECH. 9 (Apr. 2016), for an interesting discussion on the Internet of Things and a more in-depth consideration of how our household gadgets connect to one another, as well as the legal implications of that connectivity.

[91] *See* United States v. Meregildo, 883 F. Supp. 2d 523, 525–26 (S.D.N.Y. 2012); Adrian Fontecilla, *The Ascendance of Social Media as Evidence*, 28 CRIM. JUST. 55, 56 (Spring 2013).

[92] United States v. Katz, 389 U.S. 347, 353 (1967).

Physician-prescribed wearable devices present different issues.[93] Privacy interests in health information extend far beyond physical intrusions like searches and seizures, often involving a vast array of more specific interests (e.g., the interest in disclosing personal matters and the interest in having autonomy to make decisions about one's body and health).[94] Wearable technology, especially physician-prescribed devices, implicate these concerns by gathering and storing healthcare information—information traditionally seen as deserving of Fourth Amendment protections.[95] Once a legitimate expectation of privacy is identified, the court must weigh "the asserted government interest against the specific intrusion of privacy."[96] Several factors are taken into consideration, such as the uses to which the individual has put the information, and "a societal understanding that certain areas deserve the most scrupulous protection from government invasion."[97]

The Health Insurance Portability and Accountability Act (HIPAA), often cited as a possible source of data privacy protections,[98] does not currently protect data created by voluntary use of wearable devices.[99]

HIPAA and state health privacy laws generally only cover the activities of certain medical entities and 'business associates' that work with them.[100] Wearable technology manufacturers are not a 'covered entity' under HIPAA, and even if they were, there's an exception to this law for law enforcement inquiries, national security needs, and a number of other legal requests.[101]

Moreover, without any judicial oversight, HIPAA allows law enforcement to use written requests to obtain medical information, provided

---

[93] Devon T. Unger, Note, *Minding Your Meds: Balancing the Needs for Patient Privacy and Law Enforcement in Prescription Drug Monitoring Programs*, 117 W. VA. L. REV. 345, 357 (2014) ("Courts have typically held that individuals have a legitimate expectation of privacy in their healthcare information.").

[94] Whalen v. Roe, 429 U.S. 589, 599–600 (1977); *see also* Unger, supra note 93, at 355 (citing Roe, 429 U.S. at 599–600). Consider a reality where health insurance companies can base premiums on how many vegetables you eat. *See* Denise Johnson, *How Wearable Devices Could Disrupt the Insurance Industry*, INS. J. (May 6, 2015), http://www.insurancejournal.com/news/national/2015/05/06/367014.htm.

[95] *See* Unger, *supra* note 93, at 355.

[96] *Id.* at 357 (citing Nat'l Treasury Emps. Union v. Von Raab, 489 U.S. 656, 671 (1989)).

[97] *See* Oliver v. United States, 466 U.S. 170, 178 (1984).

[98] *See, e.g.*, Nicole Chauriye, Note, *Wearable Devices as Admissible Evidence: Technology is Killing Our Opportunities to Lie*, 24 CATH. U.J.L. & TECH. 495, 505–06 (2016); Gregory James Evans, *Regulating Data Practices: How State Laws Can Shore Up the FTC's Authority to Regulate Data Breaches, Privacy, and More*, 67 ADMIN. L. REV. 187, 219 (2015); Antigone Peyton, *The Connected State of Things: A Lawyer's Survival Guide in an Internet of Things World*, 24 CATH. U. J. L. & TECH. 369, 379 (Spring 2016); Drew Simshaw et. al., *Regulating Healthcare Robots: Maximizing Opportunities While Minimizing Risks*, 22 RICH. J.L. & TECH. 3, 51 (2016).

[99] Chauriye, *supra* note 98.

[100] Peyton, *supra* note 98, at 379.

[101] *Id.*

they make assurances that the information is "relevant, material, and limited in scope, and that masked information is insufficient."[102] The patient's authorization is not required, and individuals are notified after-the-fact about police access via a generic notice of privacy procedures.[103]

Given the feigned and minimal protections offered by HIPAA, the distinction between medically-prescribed devices and consumer gadgets is arbitrary and potentially more harmful to personal liberty than helpful. A more useful and long-lasting approach would be for courts to consider a generalized rule that would apply to all digital data.

B. Fifth Amendment Questions

"No person . . . shall be compelled in any criminal case to be a witness against himself . . . ."[104] The Fifth Amendment's relevance to the issues presented by wearable tech is no less convoluted and nuanced than Fourth Amendment application. Fortunately, recent decisions involving encryption are proof that courts are willing to recognize a relationship between digital data and the privilege against self-incrimination.[105] In doing so, courts are slowly establishing a long-overdue legal relationship between the Fifth Amendment privilege against self-incrimination and the evolving roles of technology, digital data, and encryption.

The constitutional protection against self-incrimination was greatly diminished in 1976 with *Fischer v. United States*.[106] Self-incrimination was held not to include the compelled production of incriminating documents, meaning a person could be forced to turn over private papers if the papers were created before the incident.[107] Such documents are not "testimonial" in nature[108] and cannot be "compelled" in the sense the privilege requires.[109] A suspect can therefore be required to give a handwriting sample[110] or blood sample,[111] or stand in a lineup,[112] because such acts do not require the suspect

---

[102] *Id.*

[103] *See id.*

[104] U.S. CONST. amend. V.

[105] *See* United States v. Doe (*In re* Grand Jury Subpoena Duces Tecum), 670 F.3d 1335, 1346 (11th Cir. 2012).

[106] 425 U.S. 391; *see also* Lance Cole, *The Fifth Amendment and Compelled Production of Personal Documents After* United States v. Hubbell - *New Protection for Private Papers?*, 29 AM. J. CRIM. L. 123, 125–26 (2002).

[107] Cole, *supra* note 106, at 126.

[108] *See* United States v. Hubbell, 530 U.S. 27, 35–36 (2000).

[109] Cole, *supra* note 106, at 126; *see also Hubbell*, 530 U.S. at 35–36.

[110] *See* Gilbert v. California, 388 U.S. 263, 266–67 (1967).

[111] *See* Schmerber v. California, 384 U.S. 757, 761 (1966).

[112] *See* United States v. Wade, 388 U.S. 218, 223 (1967).

to communicate any knowledge he might have.[113] "To be testimonial, an accused's communication must itself, explicitly or implicitly, relate a factual assertion or disclose information. Only then is a person compelled to be a 'witness' against himself."[114]

In the aftermath of *Fischer*, Fifth Amendment protection for the contents of previously-created documents has essentially been eliminated.[115] But an important question remains: is there anything so private and personal that the Fifth Amendment would shield the item from compelled production?[116] The data-mining capabilities and potential interconnectivity of smart devices and wearables mean technology is downloading and preserving the most intimate details of people's lives;[117] surely such information is deserving of Fifth Amendment protection.[118]

A 2009 case illustrates how Fifth Amendment safeguards apply to digital data.[119] In December 2006, defendant Boucher crossed the U.S.–Canadian border into Vermont.[120] Customs and border protection officers directed a secondary inspection of Boucher's vehicle.[121] During the search, one of the officers found and examined a laptop located in the car's backseat.[122] Some of the files contained child pornography, and a Special Agent for Immigration and Customs Enforcement (ICE) was called in to look at the computer.[123] After obtaining a Miranda waiver, the agent asked Boucher about an inaccessible drive found on the laptop.[124] Boucher navigated to the drive and allowed the agent to begin searching.[125] The agent found several pictures and videos that appeared to be child pornography.[126] Boucher was arrested; the

---

[113] See United States v. Doe (*In re* Grand Jury Subpoena Duces Tecum), 670 F.3d 1335, 1345–46 (11th Cir. 2012), for more examples.

[114] Doe v. United States, 487 U.S. 201, 210 (1988).

[115] Even if the prosecutor cannot prove existence, possession, and authenticity, she can still eliminate the protection by seeking use or derivative use immunity. *See Doe*, 670 F.3d at 1351 n.32 (2012); Cole, *supra* note 106, at 125–26.

[116] *See* Couch v. United States, 409 U.S. 322, 350 (1973) (Marshall, J., dissenting) ("Diaries and personal letters that record only their author's personal thoughts lie at the heart of our sense of privacy.").

[117] Kellogg, *supra* note 10, at 76.

[118] *But see* Christine Hauser, *In Connecticut Murder Case, a Fitbit is a Silent Witness*, N.Y. TIMES (Apr. 27, 2017), https://www.nytimes.com/2017/04/27/nyregion/in-connecticut-murder-case-a-fitbit-is-a-silent-witness.html.

[119] *See In re* Boucher, No. 2:06-MJ-91, 2009 WL 424718 (D. Vt. Feb. 19, 2009).

[120] *Id.* at *1.

[121] *Id.*

[122] *Id.*

[123] *Id.* at *2.

[124] *Id.*

[125] *Id.*

[126] *Id.*

laptop was seized and shut down.[127] After obtaining a search warrant, the agent went back to more thoroughly examine the file but found the drive encrypted and requiring a password.[128] The grand jury subpoenaed Boucher to produce his password.[129] Boucher moved to quash the subpoena on grounds that it violated his Fifth Amendment privilege against self-incrimination.[130]

The Fifth Amendment protects against incrimination by one's "own compelled testimonial communications."[131] The act of producing the contents of something may be privileged even if the contents themselves are not.[132] If the production implies an assertion of fact (e.g., producing documents to comply with a subpoena can amount to admitting existence, control, and authenticity), it forces the accused to "disclose the contents of his mind," therein triggering the self-incrimination clause.[133] Self-incrimination protection requires the communication be compelled, testimonial, and incriminating.[134]

Although Boucher's argument in the Vermont federal court failed, the same line of reasoning may be a better fit for the privacy concerns associated with smart device data.[135] He argued that, although the contents of his laptop were not protected under the Fifth Amendment, compelling him to produce the password to *access* his laptop was barred under the self-incrimination clause.[136] Initially, the District Court focused on whether the act would be "testimonial," that is, entailing implicit statements of fact, such as admitting that evidence exists, is authentic, and is within a suspect's control.[137] The act

---

[127] *Id.*

[128] *Id.*

[129] *Id.* On appeal, the government stated that it did not actually seek the password for the encrypted drive, but rather required Boucher to produce the contents of the drive in an unencrypted format by opening the drive before the grand jury. *Id.*

[130] *Id.* at *1.

[131] Fisher v. United States, 425 U.S. 391, 409 (1976).

[132] *In re Boucher*, 2009 WL 424718, at *2 (citing United States v. Doe, 465 U.S. 605, 611–12 (1984)).

[133] *Id.* (quoting Doe v. United States, 487 U.S. 201, 211 (1988)).

[134] *Id.*; *see also* Hoffman v. United States, 341 U.S. 479, 486 (1951) (holding (1) that the self-incrimination privilege is confined to instances where the witness has reasonable cause to apprehend danger from a direct answer and (2) that it is for the court to decide whether a witness's silence is justified). Furthermore, the privilege extends not only "to answers that would in themselves support a conviction under a federal criminal statute but likewise embraces those which would furnish a link in the chain of evidence needed to prosecute the claimant . . . ." *Hoffman*, 341 U.S. at 486.

[135] In *United States v. Hubbell*, Justice Thomas, joined by Justice Scalia, articulated an inclination to "reconsider the scope and meaning of the Self-Incrimination Clause" because "the Fifth Amendment privilege protects against the compelled production not just of incriminating testimony, but of any incriminating evidence." 530 U.S. 27, 49 (2000) (Thomas, J., concurring).

[136] *In re Boucher*, 2009 WL 424718, at *2.

[137] *Id.* at *2 (citing *Hubbell*, 530 U.S. at 36 (majority opinion)).

of production may communicate incriminating facts "in two situations: (1) if the existence and location of the subpoenaed papers are unknown to the government; or (2) where production would implicitly authenticate the documents."[138]

However, to Boucher's chagrin, if the "existence and location of the documents are already known to the government," the matter is a "foregone conclusion," and "no constitutional rights are touched."[139] Because Boucher had previously allowed the agents to see some of the pornographic files on his laptop, the existence and location of the documents were already known.[140] Had Boucher not made the initial error of accessing the drive for the agents and allowing them to view the contents of some of the drive's files,[141] he might have won his argument of privilege because it would have required him to disclose the contents of his mind—the password.

In the wake of *Fischer*, the act of producing subpoenaed digital data could be protected under the self-incrimination clause if there is an expectation of privacy regarding the evidence and if the act of production is testimonial.[142] As with Boucher's inaccessible hard drive, police will often possess the device containing the data; the problem is accessing the data.[143] In some instances, users may be able to retrieve their data themselves, but in others, the developers or other third parties may be the only ones with access.[144] Sometimes, it is not even clear who actually owns the data from these devices: the user, the company collecting the data, the company storing the data, or the company analyzing the data.[145] These factors complicate society's expectation of privacy for smart devices because they aren't in line with traditional considerations.[146]

---

[138] *In re* Grand Jury Subpoena Duces Tecum Dated Oct. 29, 1992, 1 F.3d 87, 89 (2d Cir. 1993).

[139] *In re Boucher*, 2009 WL 424718, at *3 (citing Fisher v. United States, 425 U.S. 391, 409 (1976)).

[140] *Id.*

[141] *Id.*

[142] *See* John Duong, Note, *The Intersection of the Fourth and Fifth Amendments in the Context of Encrypted Personal Data at the Border*, 2 DREXEL L. REV. 313, 334–35 (2009).

[143] United States v. Lustig, 3 F. Supp. 3d 808, 816 (S.D. Cal. 2014).

[144] *See, e.g.*, Valerie Gay & Peter Leijdekkers, *Bringing Health and Fitness Data Together for Connected Health Care: Mobile Apps as Enablers of Interoperability*, J. OF MED. INTERNET RES. (Nov. 18, 2015), https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4704968.

[145] *See* Zainab Hussain, *Weary of Wearables: IP, Privacy, and Data Security Concerns*, L. PRAC. TODAY (Jan. 14, 2016), http://www.lawpracticetoday.org/article/weary-of-wearables-ip-privacy-and-data-security-concerns.

[146] Consider, for example, location, exclusivity of control, or a manifested intent to keep something private. *See generally* United States v. Katz, 389 U.S. 347 (1967); United States v. Hamdan, 891 F. Supp. 88 (E.D. N.Y. 1995), *aff'd*, 101 F.3d 686 (2d Cir. 1996); Oliver v. United States, 466 U.S. 170, 189 (1984) (Marshall, J., dissenting).

In *United States v. Doe*, the most recent Supreme Court case to address compelled decryption, the defendant was under suspicion of using his YouTube account to distribute child pornography.[147] After isolating Doe's IP address, officers obtained a warrant to "seize all digital media, as well as any encryption devices or codes necessary to access such media."[148] Two laptops and five external hard drives were seized, but forensic investigators were not able to access the encrypted drives.[149] Doe refused to comply with the subsequent grand jury subpoena requiring him to produce the contents of the drives, citing a violation of his Fifth Amendment protections.[150]

The Court's reasoning focused on the government's intended use of the evidence and whether the immunity offered by the lower court (act of production immunity without derivative use immunity) was "sufficient to meet the immunity exception of the Fifth Amendment."[151] Finding that the offered immunity was *not* as comprehensive as the protection afforded by the Fifth Amendment privilege, the Court held Doe to be justified in refusing to answer; the judgements of contempt for refusing to comply with the lower court's order were vacated.[152]

To summarize, the cases described above[153] illustrate three considerations that Courts should look for when trying to maintain a uniform standard for digital data: (1) Is the evidence testimonial? (2) When does evidence fall under the foregone conclusion exception? (3) What level of immunity is required to compel production?[154]

Instead of attempting to make the existing framework apply to the newest technology, courts should move toward a new framework that takes into account the changing technology and what it represents. The Framers never could have imagined that citizens could walk around with devices that provided them access to all of their most sensitive information—and because

---

[147] United States v. Doe (*In re* Grand Jury Subpoena Duces Tecum), 670 F.3d 1335, 1352–53 (11th Cir. 2012).

[148] *Id.* at 1339.

[149] *Id.*

[150] *Id.*

[151] Matthew J. Weber, *Warning- Weak Password: The Courts' Indecipherable Approach to Encryption and the Fifth Amendment*, 2016 U. ILL. J.L. TECH. & POL'Y 455, 455, 469 (citing *Doe*, 670 F.3d at 1349–50 (2012)).

[152] *Doe*, 670 F.3d at 1339 (2012); *see also* Weber, *supra* note 151 (citing *Doe*, 670 F.3d at 1351–53 (2012)).

[153] *See supra* notes 16, 131, 139 and accompanying text (*Fisher v. United States*); *supra* notes 119–41 and accompanying text (*In Re Boucher*); *supra* notes 147–52 and accompanying text (*United States v. Doe* (2012)).

[154] Weber, *supra* note 151, at 460.

of that, we should look to change how we interpret access to that information.[155]

The inherently private and personal nature of wearable device data—regardless of whether the device is medically prescribed or available at Wal-Mart—suggests that suspects should not be compelled to produce the passwords to their wearables. Moreover, considering the detail, volume, and connectivity of digital data from any kind of personal smart device, courts should be cautious in allowing the foregone conclusion exception to covertly undermine intended Fifth Amendment protections.[156]

C. The Confrontation Clause and Other Evidentiary Uncertainties

Sixth Amendment scenarios involving wearables and other smart devices raise fundamental "questions regarding the witness who must be available for 'confrontation.'"[157] "Is it you, your device, the manufacturer, the service provider that collects and analyzes your data, or the company that provides the algorithms used to interpret it?"[158] The goal of the Confrontation Clause is to ensure the reliability of evidence through cross-examination.[159] In *Melendez-Diaz v. Massachusetts*, the Supreme Court discussed whether certificates of analysis, sworn to by forensic analysists at a state laboratory, could be proffered at a drug trafficking trial as prima facie evidence of the substance's composition.[160] The Court found nothing inherently unique or special about scientific evidence that should allow it to bypass normal Sixth Amendment confrontation concerns.[161] Thus, a party wishing to present scientific evidence must use a witness sufficiently familiar with the processes involved to enable a defendant to engage in effective cross-examination.[162] This decision reduces the likelihood of false information going unnoticed by providing defendants with every opportunity to expose fraudulent data.[163]

---

[155] *Id.* at 483.

[156] *See infra* Part IV (discussing how the Ninth Circuit has addressed the foregone conclusion exception).

[157] Peyton, *supra* note 98, at 398.

[158] *Id.*

[159] Crawford v. Washington, 541 U.S. 36, 61 (2004); *see also* Laura Bowzer, Melendez-Diaz v. Massachusetts*: Upholding the Goals and Guarantees of the Confrontation Clause*, 88 DENV. U. L. REV. 271, 280 (2010).

[160] Melendez-Diaz v. Massachusetts, 557 U.S. 305, 306 (2009).

[161] Bowzer, *supra* note 159, at 280–82.

[162] *Id.*

[163] "[J]uries will receive information regarding an analyst's proficiency, a machine's calibration, and a lab's reputation. Confrontation may even lead to the discovery that no testing was ever performed on the substance at issue. Conversely, cross-examination may reveal that a lab had a 99.9% accuracy rate and employed the most esteemed analysts in the country. Either way, the trier of fact will gain more

More recently, in *Pendergrass v. State*, a supervisor at a laboratory gave live testimony about DNA certificates of analysis per the *Melendez-Diaz* ruling.[164] Pendergrass was convicted, and he appealed on Sixth Amendment grounds, arguing that the testimony should have been given by the analyst who conducted the test.[165] The conviction was upheld by the Supreme Court of Indiana.[166] The United States Supreme Court denied certiorari.[167] Accordingly, "the analyst offering live testimony should be one who is in a position to testify to the general and specific scientific procedures that lead to the data submitted as evidence against the defendant."[168] This distinction becomes important when courts must decide who will confront a defendant with incriminating, user-created data.

In *Williams v. Illinois*, Justice Alito, writing for the plurality, applied the testimonial distinction to DNA evidence when he found that an expert could testify as to "others' testimonial statements if those statements are not themselves admitted as evidence."[169] In support of this imprecise argument, the Court reasoned that "the inadmissibility of the underlying testimonial evidence could be isolated from the expert's reliance upon them."[170]

Justice Kennedy's dissent in *Melendez-Diaz* noted the logistical problems that would arise from requiring lab technician testimony for all digital data, writing that it would be a "windfall to defendants" to hinge prosecutions on such requirements.[171] The magnitude of data being created in modern society underscores their words.[172] If courts continue to ignore this proliferation, entities following the *Williams* decision "that generate forensic data" could "simply produce unsigned reports that do not identify the technician who ran the test or the analyst who compiled the data."[173] Justice

---

information about the evidence brought against the defendant, and will therefore have a deeper understanding about that evidence's reliability." Bowzer, *supra* note 159, at 281–82 (internal citations omitted).

[164] Pendergrass v. State, 913 N.E.2d 703, 703–04 (Ind. 2009), *abrogated by* Speers v. State, 999 N.E.2d 850 (Ind. 2013).

[165] *Id.* at 704.

[166] *Id.* at 709.

[167] *See* Pendergrass v. Indiana, 560 U.S. 965 (2010).

[168] Bowzer, *supra* note 159, at 286.

[169] Williams v. Illinois, 567 U.S. 50, 56 (2012) (plurality opinion).

[170] Merritt Baer, *Who Is the Witness to an Internet Crime: The Confrontation Clause, Digital Forensics, and Child Pornography*, 30 SANTA CLARA HIGH TECH. L. J. 31, 40 (2013) (citing *Williams*, 567 U.S. at 63).

[171] *Id.* at 46–47 (citing Melendez-Diaz v. Massachusetts, 557 U.S. 305, 306 (2009) (Kennedy, J., dissenting)).

[172] According to IBM, in 2012, 2.5 billion gigabytes of data were generated every day. Matthew Wall, *Big Data: Are You Ready for Blast-Off?*, BBC NEWS (Mar. 4, 2014), http://www.bbc.com/news/business-26383058.

[173] Baer, *supra* note 170, at 48 (citing *Williams*, 132 S. Ct. at 2276 (Kagan, J., dissenting)).

Alito in *Williams* asserted that the DNA report was not intended as evidence against the defendant and thus invoked no right to confrontation.[174] In her dissent, Justice Kagan expressed the opinion that it would not take long for the government to develop whatever magic words necessary so as to never call anything a "certificate" again.[175]

Setting aside the issues of authentication, one solution to the difficulty of classifying information from wearable devices is to hold that all digital data sought to be introduced as evidence should be considered hearsay pursuant to the Federal Rules of Evidence ("FRE").[176] Such a rule would help address the "mutable and untestable nature" of user-created data by requiring an "affirmative showing of reliability."[177] Hearsay is any statement by an out-of-court declarant, offered to prove the truth of the matter asserted.[178] Once hearsay evidence is authenticated under Rule 901, it must fall under an exception to be admissible; each rule thus occupies "sequential yet co-equal conditions to admissibility."[179]

Currently, the FRE defines a declarant as a "person who made the statement."[180] A literal translation of "person" precludes wearable device data from being classified as hearsay.[181] However, if courts ignore the problem of semantics in favor of an interpretation based on logical assumptions, then a credible argument can be made that "all digital data constitutes some type of hearsay."[182] By recognizing that digital data of any type consists of statements made by either the device designer or by the user, then it follows that if the intended result of these assertions is to have the content read or viewed, the declarations fall within the purview of hearsay.[183]

In addition to Confrontation Clause concerns, there are other evidentiary issues complicated by the intangible nature of digital data.[184] The process of discovering, seizing, and interpreting digital evidence is different from traditional law enforcement practices because it is the contents of the device

---

[174] *Williams*, 132 S. Ct. at 2224, 2226 (plurality opinion).

[175] *Id.* at 2276 (Kagan, J., dissenting).

[176] *See* Steven W. Teppler, *Testable Reliability: A Modernized Approach to ESI Admissibility*, 12 AVE MARIA L. REV. 213, 215-16 (2014).

[177] *Id.* at 214.

[178] *Id.* at 229.

[179] *Id.* at 225.

[180] FED. R. EVID. 801(b).

[181] Teppler, *supra* note 176, at 229–30.

[182] *Id.* at 231.

[183] *Id.* at 233.

[184] *See* Joshua Eames, *Criminal Procedure – "Can You Hear Me Now?": Warrantless Cell Phone Searches and the Fourth Amendment;* People v. Diaz, *244 P.3d 501 (Cal. 2011)*, 12 WYO. L. REV. 483, 499–501 (2012).

rather than the device itself which is of significance.[185] Under federal constitutional law, when law enforcement obtains a warrant, the items to be seized and their location must be described with "particularity."[186] This becomes inherently more difficult when the information is stored and shared between an array of companies and devices.[187]

Reliability is another concern. Fitbit is currently defending itself against two lawsuits in the Northern District of California, both alleging that Fitbit's heartrate monitoring system is dangerously inaccurate and poses serious health risks to consumers.[188] There are also concerns about the authenticity of such data and a general lack of standardization if the user takes the device off, forgets to charge it, or lends it to a friend.[189] Moreover, there is a risk juries will give more credibility to wearable device data than to a witness's own sensory impressions.[190] Good or bad, this is another balancing test courts will have to grapple with.[191] Judges and juries will need to be made aware of the limitations and imperfections associated with the information, as well as whether there are any interpretive aspects in how the data is formulated.[192]

IV. POLICY RECOMMENDATIONS

The recent efforts of an Arkansas prosecutor to obtain data from Amazon's voice-activated digital assistant, Echo, provide a near-perfect framework to consider how these issues are likely to play out in state courts. The Amazon Echo is a 9.3-inch smart-speaker that connects with the voice-controlled digital service Alexa and is capable of music playback, streaming podcasts and audiobooks, making to-do lists, setting alarms, and providing

---

[185] Orin S. Kerr, *Digital Evidence and the New Criminal Procedure*, 105 COLUM. L. REV. 279, 300 (2005).

[186] *See* McDonald v. United States, 335 U.S. 451, 453 (1948).

[187] Kellogg, *supra* note 10, at 77 ("A Federal Trade Commission (FTC) study released in May 2014 revealed that 12 mobile health applications and devices transmitted information to 76 different third parties, and some of the data could be linked back to specific users. In addition, 18 third parties received device-specific identifiers, 14 received consumer-specific identifiers, and 22 received other key health information.").

[188] Robb v. Fitbit Inc., 216 F.Supp.3d 1017, 1023 (N.D. Cal. 2016) (citing McLellan et al. v. Fitbit, Inc., 3:16-cv-00036-JD (N.D. Cal. Jan. 5, 2016)).

[189] Kellogg, *supra* note 10, at 82.

[190] *See* Peyton, *supra* note 90, at 19 (describing Fitbit's sleep analysis programs, how they use algorithms based on typical user data, and the impact they could have on a compensation claim where one party is accused of being sleep-deprived).

[191] *Compare* Kristin Bergman, *Cyborgs in the Courtroom: The Use of Google Glass Recordings in Litigation*, 20 RICH. J.L. & TECH. 11, 29 (2014) (stating that data from wearable tech could solve some of the typical problems associated with "witness credibility," such as "bias and memory issues"), *with* Chauriye, *supra* note 98, at 517 (discussing the "unique weight" expert testimony can have on juries).

[192] Peyton, *supra* note 90, at 20, 32.

weather, traffic, and other real-time information.[193] Echo can also act as a home automation hub by interfacing with various other smart devices.[194]

Most alarmingly perhaps, the Echo device is always on and always listening, responding to a "wake word" when a user wants to activate a service.[195] "From the moment you wake up Echo to the end of your command, your voice is recorded and transcribed."[196] These transcripts are stored on Amazon servers, where the company says the data is used to improve the product.[197]

In November 2015, 47-year-old Victor Collins was found dead, floating face down in a friend's hot tub.[198] The friend and home owner, 31-year-old James Bates, told police he and Collins had been hanging out with friends and drinking the night before.[199] Bates asserts that when he went to bed, everything was fine; Collins and another friend were still in the hot tub.[200] Bates stated that the next morning, he opened his backdoor, saw Collins' body in the hot tub, and called 9-1-1.[201] Detectives described Collins as having a black eye, cuts and bruises, and blood coming from his mouth and nose; it also appeared the rim of the hot tub and the surrounding patio had been sprayed off.[202] Bates was arrested for first-degree murder on February 22, 2016.[203] His attorney, Kimberly Weber, asserts Collins' death was an accident stemming from his drinking; Collins' blood-alcohol content at the time of death was 0.32.[204]

The Amazon Echo became of interest to the prosecution when someone present the night of Collins' death recalled hearing music through the device.[205] Police served a warrant on Amazon seeking "all audio recordings,

---

[193] *Amazon Echo*, AMAZON, https://www.amazon.com/Amazon-Echo-Bluetooth-Speaker-with-WiFi-Alexa/dp/B00X4WHP5E (click "Technical details" to scroll to relevant information) (last visited Feb. 1, 2017).

[194] *Id.* (see main product description).

[195] Profis, *supra* note 41.

[196] *Id.*

[197] *Id.*

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

[199] *Id.*

[200] *Id.*

[201] *Id.*

[202] *Id.*

[203] *Id.*

[204] Elliot C. McLaughlin & Keith Allen, *Alexa, Can You Help With This Murder Case?*, CNN (Dec. 28, 2016, 8:48 PM), http://www.cnn.com/2016/12/28/tech/amazon-echo-alexa-bentonville-arkansas-murder-case-trnd.

[205] *Id.*

transcribed records, text records and other data" from Bates' device.[206] So far, Amazon has refused to hand over anything more than Bates' account details and purchase history, stating: "Amazon will not release customer information without a valid and binding legal demand properly served on us. Amazon objects to overbroad or otherwise inappropriate demands as a matter of course."[207]

Although the Amazon Echo is not a wearable device, the information it creates and stores raises similar privacy concerns as data from a Fitbit or similar gadget. So what would "a valid and binding legal demand" look like?[208] Many argue that the analysis in *Riley* should be broadened to extend to all mobile digital devices.[209] Like cell phones, the digital data created by a Fitbit or Amazon Echo Dot[210] would be entirely excluded from the search-incident-to-arrest exception.[211]

While *Riley* is a good starting part, this Note suggests that an even broader standard should be required. Traditional standards of privacy—wherein homes, bodily autonomy, and mental processes fit into special zones and deserve the highest protections—still apply. But these zones need to be expanded and analogized to conform with the realities of modern technology. Devices like Fitbit that monitor personal health information and gadgets like Amazon Echo that improve the comfort of one's home impact a whole new level of personal invasion that could not have been conceived of when the Constitution was framed. By redefining our expectations of privacy to include these expansions of traditional spheres, courts can maintain the original intent of the Framers and still adapt to the demands of modern technology.

Traditional search warrants are limited by time, place, and particular items; thus, law enforcement can seize items they have specified and any other illegal items in plain view.[212] Although *Riley* was specific to cell phones, the language used by Chief Justice Roberts "commented extensively

---

[206] Jill Bleed, *Alexa a Witness to Murder? Prosecutors Seek Amazon Echo Data*, CNS NEWS (Dec. 28, 2016, 5:00 PM), http://www.cnsnews.com/news/article/alexa-witness-murder-prosecutors-seek-amazon-echo-data (internal quotation marks omitted).

[207] Billy Steele, *Police Seek Amazon Echo Data in Murder Case*, ENGADGET (Dec. 27, 2016), https://www.engadget.com/2016/12/27/amazon-echo-audio-data-murder-case.

[208] *Id.*

[209] *See* Ellis, *supra* note 68, at 469; Kylie J. Brown & Carol M. Bast, *The Constitutionality of Warrantless Cell Phone Searches Incident to Arrest*, 52 CRIM. L. BULL. 6 (Winter 2016).

[210] The Echo Dot is the mobile version of the Echo. *See Echo Dot*, AMAZON, https://www.amazon.com/All-New-Amazon-Echo-Dot-Add-Alexa-To-Any-Room/dp/B01DFKC2SO (last visited Aug. 6, 2017).

[211] Ellis, *supra* note 68, at 492.

[212] Nathan E. Carrell, *Spying on the Mob: United States v. Scarfo - A Constitutional Analysis*, 2002 U. ILL. J.L. TECH. & POL'Y 193, 201–02 (2002).

on individual interests at stake when the government searches digital devices."[213] Accordingly, devices producing digital data should not be thought of as containers,[214] nor should they be subject to the traditional plain view doctrine.[215]

The Ninth Circuit has entirely rejected the plain view doctrine with regard to the seizure of digital data, holding that before a judge can sign a warrant for police to examine a computer hard drive or electronic storage medium, the government must waive reliance on the plain view doctrine entirely, allow third-party segregation and redaction of information, disclose the risk of destruction to information, disclose any prior attempts to seize that information, limit search protocols to information for which it has probable cause, and destroy or return non-responsive data.[216]

The Ninth Circuit's rule on seizure of digital data shows the need for states to take great care in revising current laws to address this issue. As stated previously, this Note advocates for broad, overarching classifications for digital data; that is, classifications that do not distinguish between wearable devices, home automation hubs, smart phones, laptops, medically prescribed biometrics, or any other gadget capable of collecting and producing user data. The following model statute provides this kind of broad categorization while maintaining specificity in its terms and definitions:

Model Digital Data Privacy Act

§ 1 – The purpose of this statute is to specify what will be required of a warrant to search and seize digital data.

---

[213] *See* Thomas K. Clancy, *Fourth Amendment Satisfaction-the "Reasonableness" of Digital Searches*, 48 TEX. TECH L. REV. 37, 49 (2015).

[214] State v. Smith, 920 N.E.2d 949, 954 (Ohio 2009) ("We acknowledge that some federal courts have likened electronic devices to closed containers. Each of these cases, however, fails to consider the Supreme Court's definition of 'container' in Belton, which implies that the container must actually have a physical object within it. Additionally, the pagers and computer memo books of the early and mid 1990s bear little resemblance to the cell phones of today. Even the more basic models of modern cell phones are capable of storing a wealth of digitized information wholly unlike any physical object found within a closed container. We thus hold that a cell phone is not a closed container for purposes of a Fourth Amendment analysis.") (citations omitted).

[215] Kate Brueggemann Ward, *The Plain (or Not So Plain) View Doctrine: Applying the Plain View Doctrine to Digital Seizures*, 79 U. CIN. L. REV. 1163, 1178 (2011) ("[T]he problem with searches and seizures of computer and digital devices is there is no way to know exactly what a file contains unless the file is opened and its contents revealed. Specifically, necessary efforts to locate particular files requires examining a great many other files to exclude the possibility that the sought-after data is concealed in those other files. Once a file is examined, however, the government may claim that the contents are in plain view, and if incriminating, may keep it, which allows for over-seizing. In order to solve this problem, the Ninth Circuit eliminated the plain view doctrine in cases involving digital evidence and adopted a special standard.")

[216] *See generally* United States v. Comprehensive Drug Testing, Inc., 579 F.3d 989 (9th Cir. 2009), *modified on reh'g*, 621 F.3d 1162 (9th Cir. 2010); Ward, *supra* note 215, at 1178–79.

§ 2 – Key Terms.
§ 2A – Digital Data: discrete, discontinuous representations of information or works, as contrasted with continuous, or analog signals, which behave in a continuous manner
§ 2B – Prosecuting Agency: any governmental or administrative agency involved in the investigation or prosecution of a criminal defendant
§ 2C – Neutral Third-Party: a party that is not invested in any way in the outcome of the search or seizure
§ 2D – Preponderance of Evidence: requires that a desired inference be more probable than not
§ 3 – The prosecuting agency must waive all plain-view doctrine exceptions.
§ 4 – Search protocols must be limited to gathering only information for which the searcher can demonstrate a preponderance of evidence. This must be demonstrated to a neutral magistrate.
§ 5 – Failure to comply in all respects with this statute will result in the unilateral suppression of any improperly obtained digital data.
§ 6 – Under no circumstances should the contents of any digital data device be exploited for purposes of profit, publication, or distribution; violations will carry a mandatory fine and prison sentence.
§ 7 – Any person who, under color of statute, subjects a citizen to a deprivation of privacy through the search and seizure of digital device data shall be liable to the party injured in action at law, a suit in equity, or any other appropriate procedure for redress.

This model statute provides a clear and highly restrictive framework for searches pertaining to digital evidence. Like the Ninth Circuit,[217] Section 3 eliminates the plain view exception. Because law enforcement often have to search a device extensively to locate whatever specific files are being sought, the possibility of over-seizing data in "plain view" is too grave to allow this exception to apply to digital data.

Section 4 demands a "more likely than not" standard rather than mere probable cause. The advent of industry 4.0 means an unprecedented level of connectivity between our devices, so that accessing one could mean access to every private file traditionally kept locked away in desk drawers and cabinets back home. The potential for abuse is simply too great to allow anything less than a preponderance of evidence standard for justifying searches of smart device data.

Likewise, section 5 adds another layer of protection. By embodying the exclusionary rule so that any evidence obtained outside the scope of the model statue would be unilaterally suppressed, the hope is to "compel respect

---

[217] *See generally Comprehensive Drug Testing, Inc.*, 579 F.3d 989.

for the constitutional guarantee [of the Fourth Amendment] in the only effectively available way – by removing the incentive to disregard it."[218]

Sections 6 and 7 provide remedies to citizens whose privacy has been violated under the model statute. By detailing unambiguous sanctions for violations of the statute's specifications, citizens are given the legal recourse to pursue criminal or civil redress for privacy abuses. By adopting regulations resembling the model statute, states would avoid many of the problems presented by digital data.

V. CONCLUSION

Although wearable technology has been the framework for considering many of these issues, this Note does not call for special rules for special devices, but rather hopes to encourage courts to reconsider rules of general application. Distinctions can be made between medically prescribed devices and consumer gadgets, mobile technology and home automation devices like Amazon Echo, smart phones and tablets—but the reality is that the world is becoming more and more connected, and soon, regardless of the actual device, every gadget will be networked in some way to everything else. Such distinctions become useless when taken to their logical conclusions.

Three important reasons exist for establishing strict privacy parameters for digital data. First and foremost is the Fourth Amendment right to be free from unreasonable searches. The harm from unreasonable searches "is not the breaking of his doors, and the rummaging of his drawers," but rather "the invasion of his indefeasible right of personal security, personal liberty and private property, where that right has never been forfeited by his conviction of some public offense . . . ."[219] The inherently personal nature of most smart device data ensures that any invasion, even when made in good faith, has potential repercussions.

Another reason for creating uniformity stems from the doctrine of qualified immunity. Those individuals wishing to vindicate their rights after an unreasonable search have no real recourse until it can be said that such searches violate "clearly established statutory or constitutional rights of which a reasonable person would have known."[220]

Relatedly, one of the ways courts deter unconstitutional searches is through the Supreme Court-created exclusionary rule, which "bars the

---

[218] Elkins v. United States, 364 U.S. 206, 217 (1960).

[219] Boyd v. United States, 116 U.S. 616, 630 (1886).

[220] Newhard v. Borders, 649 F. Supp. 2d 440, 447 (W.D. Va. 2009) (internal quotation marks and citations omitted).

prosecution from introducing evidence obtained by way of a Fourth Amendment violation."[221] However, the "good faith exception" means that evidence will not be excluded unless "a reasonably well trained officer would have known that the search was illegal in light of all the circumstances."[222] This exception highlights the need for precision and unambiguity when regulating how constitutional protections apply to digital data.

The inconsistent applications of the Fourth, Fifth, and Sixth Amendments to wearable technology and other smart devices make clear how badly a bright-line determination is needed. Courts should be proactive in crafting new rules to be applied to digital data in anticipation of future advancements. Moreover, these new rules have a place among traditional understandings of zones of privacy, self-incrimination, and the Confrontation Clause.

---

[221] Davis v. United States, 564 U.S. 229, 232 (2011).

[222] Ellis, *supra* note 68, at 481 (internal quotation marks and citations omitted). Consider also that the Fifth Amendment has a similar "foregone conclusion" exception. *See* Weber, *supra* note 151, at 462.