Catholic University Journal of Law and Technology

Volume 24 | Issue 2 Article 9

2016

Wearable Devices as Admissible Evidence: Technology is Killing Our Opportunity to Lie

Nicole Chauriye
Catholic University of America, Columbus School of Law

WEARABLE DEVICES AS ADMISSIBLE EVIDENCE: TECHNOLOGY IS KILLING OUR OPPORTUNITIES TO LIE

Nicole Chauriye*

> "Every giant leap for mankind resulting from a technological advance requires a commensurate step in the opposite direction - a counterweight to ground us in humanity."[1]
>
> -Alex Morritt, author, poet, lyricist, & indie publisher

I. INTRODUCTION

The use of wearable technology such as smart watches, activity trackers, GPS-connected devices, and other "personal" monitoring devices is on the rise and it is beginning to invade what is left of our privacy. [2] Although wearable technology is marketed for its health and exercise benefits,[3] the widespread use of this type of mobile technology is becoming a tool used by attorneys and considered by courts.[4] In establishing case law on this matter, courts must strike a balance between the benefits of such technology and people's expectation of privacy.[5] One of the first cases to to test this balance involves a criminal

* J.D. Candidate 2016, The Catholic University of America: Columbus School of Law; B.A. 2011, Pennsylvania State University. The author would like to thank Professor Mary Leary for all her invaluable legal insight on this Comment and the editorial board of the *Catholic University of Law and Technology* for all of their assistance in the writing and editing process. The author would also like to thank her family and friends for all of their emotional support through the law school process.

1 Alex Morritt, *Impromptu Scribe*, http://bit.ly/1OT0S65 (last visited April 15, 2016).

2 Phil Johnson, *Loss of Privacy is the Top Concern about Wearables*, IT WORLD (April 28, 2015) http://bit.ly/1TrPTTf.

3 David Pogue, *Wearable Devices Nudge You to Health*, N.Y. TIMES (June 26, 2013), http://nyti.ms/1XshvXI.

4 *See* Kate Pickles, *Police Claim Woman Lied About Being Raped After Her 'Fitbit' Fitness Watch Showed She Had Not Been Dragged From Her Bed*, DAILY MAIL (June 22, 2015, 9:47 AM), http://dailym.ai/1YSPHux (discussing how the data retrieved from a woman's wearable technology were inconsistent with her claims of sexual assault).

5 *See* CCS INSIGHT, GLOBAL WEARABLES FORECAST, 2015-2019 (2015),

defendant who was "wrongfully" charged with sexual assult.[6] This case is only the first in what is likely to be a tidal wave of lawsuits in which digital data produced by wearable technology will serve as key evidence. Courts will likely have to grapple with the validity, admissibility, and practicaibility of using wearable technology in a given case.

The focus of this Comment's discusssion is a Pennsylvania criminal case at the trial-level, *Commonwealth v. Risley*. In *Risley*, the police questioned a woman's rape claim when her Fitbit contradicted her statement to the police.[7] Ms. Jeannine Risley is now facing three misdemeanor counts for prompting an emergency response and manhunt in response to her allegations.[8] However, the pivotal questions involving wearable technology are: what category of technology does a Fitbit fall under as it affects privacy rights, and whether police use of a Fitbit's data should be permissible against the alleged victim.

Fitbit's privacy policies "seem to allow [the Fitbit Corporation] to share [users'] data with third parties, if they so choose."[9] 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."[10] The enormous value of such technology has even been noticed by the Central Intelligence Agency, who see one potential use as identifying an individual with 100% certainty based solely on their gait, or how they walk.[11]

Maintaining a more nutritious diet and getting in better physical shape have become a recent fitness trend.[12] New technologies compliment this trend by creating wearable devices that measure an individual's calorie consumption and daily physical activity.[13] These devices offer a person a sense of control

---

http://bit.ly/1WL2Bg3 ("245 million wearable devices will be sold in 2019, up from 84 million in 2015").

[6] Commonwealth v. Risley, Criminal Docket: CP-36-CR-0002937-2015 (Lancaster Cty., Pa., printed Nov. 16, 2015).

[7] *Id.*; *see also* Pickles, *supra* note 4.

[8] Pickles, *supra* note 4.

[9] Justin Sedor, *Fitbit, Nike, & Jawbone Could Soon Be Selling Your Fitness Data*, REFINERY29 (Jan. 31, 2014, 1:15 PM), http://r29.co/1TSxdGx (quoting CIA Chief Technology Officer, Ira Hunt).

[10] *Id.*

[11] *Id*.

[12] *See* JESSICA E. TODD, U.S.DEP'T OF AGRICULTURE, ECON. RES. RPT. NO. 161, CHANGES IN EATING PATTERNS AND DIET QUALITY AMONG WORKING-AGE ADULTS, 2005-2010, at 10 (2014), http://1.usa.gov/25isVU0 (finding Americans consume less calories from foods containing saturated fats); Press Release, Rebecca Riffkin, Gallup, So Far in 2015, More Americans Exercising Frequently (July 29, 2015), http://bit.ly/25cl2fs (reporting Americans are exercising more weekly than in recent years).

[13] Adam Steele, *An Emergency Room in Your Living Room: Privacy Concerns as Health Information Moves Outside of the Traditional Medical Provider Context*, 19 VA. J.L.

over their lives. Wearable technology "collect[s] data about a user's steps walked, calories burned, activity intensity, sleep, and other health and fitness metrics … devices also connect to the internet … allow[ing] the user to view and analyze the data collected . . . "[14] However, this sense of control can easily cross the line into a privacy violation, or an illegal police search or seizure when such data is accessed by third parties.[15]

One way in which wearable technology creates a privacy concern arises from its capability of functioning as a personal GPS device.[16] More recently, those in the legal field are increasingly concerned with how data generated by wearable technology will be used, if at all, as a source of information in litigation and in the discovery process.[17] Chief Justice John G. Roberts of the United States Supreme Court recently remarked:

what if you have a device that doesn't have the broad information that a smartphone has, but only a very limited, like a Fitbit that tells you how many steps you've taken, and the defendant says, I've been in my house all afternoon, and they want to check and see if he's walked 4 miles.[18]

Chief Justice Robert's concern reflects the current ambiguity on the legal questions surrounding wearable technology, and the data it produces, as evidence. Furthermore, this ambiguity was reflected in the *Risley* case because the rape allegation in that case was contradicted by data discovered through the victim's Fitbit. Responses to the Risley incident have been drastic, one commenter went as far as to say that "if you're going to fake a rape, remember to take off your Fitbit."[19] Although wearable technology presents many legal issues, this Comment will examine what policy should be adopted for the admissibility of these devices as evidence.

This Comment will focus on Fitbits, however, the analysis is intended to be broad and analogous to suggest a solution for most wearable technology. The

---

& TECH. 388, 402 (2015).

14 Fitbug Ltd. v. Fitbit, Inc., 2015 U.S. Dist. Lexis 73325 at *3-4 (N.D. Cal. June 5, 2015).

15 *But see* Smith v. Maryland, 442 U.S. 735, 745 (1979) (holding individuals do not have a reasonable expectation of privacy in information voluntarily conveyed to third parties).

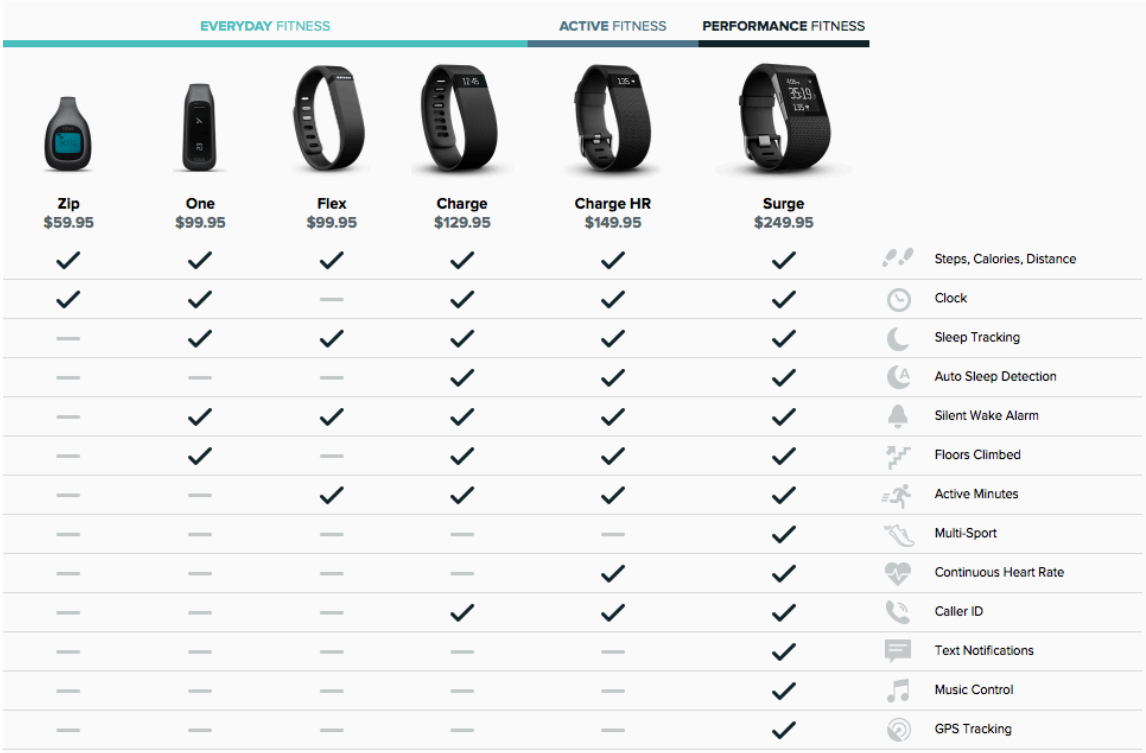
16 *See* Amber Hunt, *Experts: Wearable Tech Tests Our Privacy Limits*, USA TODAY (Feb. 5, 2015, 9:32 PM), http://usat.ly/1XshPpt ("Some wearables contain location-based personally identifiable information, allowing outsiders who gain access to see where you are in real time.").

17 *See* Kate Crawford, *When Fitbit Is the Expert Witness,* THE ATLANTIC (Nov. 19, 2014), http://theatln.tc/22fb92A (detailing a Canadian lawsuit where the plaintiff is using her Fitbit data to prove personal injury).

18 Transcript of Oral Argument at 17, Riley v. California, 573 U.S. ___, 134 S.Ct. 2473 (2014) (No. 13-132).

19 *See, e.g.*, Jim Treacher, *If You're Going To Fake A Rape, Remember To Take Off Your Fitbit,* DAILY CALLER (June 19, 2015, 12:53 PM), http://bit.ly/22mmEBC.

Fitbit Corporation[20] produces various models of these devices, which measure various personal items such as GPS tracking, sleep tracking, and your movements, as illustrated in the following chart.[21]



	EVERYDAY FITNESS				ACTIVE FITNESS	PERFORMANCE FITNESS	
	Zip $59.95	One $99.95	Flex $99.95	Charge $129.95	Charge HR $149.95	Surge $249.95	
	✓	✓	✓	✓	✓	✓	Steps, Calories, Distance
	✓	✓	—	✓	✓	✓	Clock
	—	✓	✓	✓	✓	✓	Sleep Tracking
	—	—	—	✓	✓	✓	Auto Sleep Detection
	—	✓	✓	✓	✓	✓	Silent Wake Alarm
	—	✓	—	✓	✓	✓	Floors Climbed
	—	—	✓	✓	✓	✓	Active Minutes
	—	—	—	—	—	✓	Multi-Sport
	—	—	—	—	✓	✓	Continuous Heart Rate
	—	—	—	✓	✓	✓	Caller ID
	—	—	—	—	—	✓	Text Notifications
	—	—	—	—	—	✓	Music Control
	—	—	—	—	—	✓	GPS Tracking

This Comment advocates for a strict set of rules regarding the search, seizure, and admissibility of data obtained from a wearable technology as evidence. Part I discusses the basic technological and legal information involved with Fitbits and other similar wearable technology. Part II examines the need to adopt legislation that establishes evidentiary rules to address Fitbits. This Comment analyzes these issues in the context of a Pennsylvania case where an alleged rape accusation was dismissed due to contradictory evidence obtained by police from the victim's Fitbit.[22] Part III discusses the current rules of evidence and the legal ambiguities created by the wearable technology sector. Part

---

20 *Who We Are*, FITBIT, http://fitbit.link/1sydwgI (last visited Feb. 1, 2016).

21 Ari Jay Comet, *BATTLE! – Fitbit Surge Versus Fitbit Charge HR (Heart Rate) Versus Jawbone UP3 Versus Apple Watch Versus The Competition*, ARI JAY COMET: BLOG (Jan. 25, 2015), http://bit.ly/1NHGtkf.

22 *See e.g.* Treacher, *supra* note 19.

IV of this Comment presents an advisory set of evidentiary rules for Fitbits in regards to police warrants, searches, seizures, and court admissibility. Finally, Part V will review the arguments discussed and suggest the direction that this controversial topic should move forward, and how this evidence ought to be used by law enforcement and the courts.

II. CURRENT FITBIT AND WEARABLE TECHNOLOGY INFORMATION

A. Wearable Technology

Wearable technology is "a category of technology devices that can be worn by a consumer and often include[s] tracking information related to health and fitness . . . [and] include[s] devices that have small motion sensors to take photos and sync with your mobile devices."[23] With the constant improvement of technology, these devices are not just watches that tell the owner the time of day but rather a "device coupled with sensors and data gathering capabilities contained within an integrated system worn by a person."[24] Wearable technology, such as a Fitbit, collects vast amounts of valuable information about their users.[25] Wearable technology devices "are clothing and accessories that incorporate computers, cameras and other forms of electronic technologies … [and] are generally more sophisticated" than any of those technologies individually.[26] Essentially a Fitbit is a "bracelet that contains an accelerometer, which is a device that senses its wearer's movements … [and] also measure[s] sleep patterns."[27] Other forms of this wearable technology include: Apple Watches,[28] Tile Item trackers,[29] Garmin Vivo Smart HR Activity Tracker,[30] Samsung

---

[23] Vangie Beal, *Wearable Technology*, WEBOPEDIA, http://bit.ly/1U7dylL (last visited Feb. 25, 2016); *see also* Anjanette H. Raymond & Scott J. Shackelford, *Jury Glasses: Wearable Technology and Its Role In Crowdsourcing Justice*, 17 CARDOZO J. CONFLICT RESOL. 115, 121 (2015) (". . . wearable technology is more than a mere smart watch, but instead is a device coupled with sensors and data gathering capabilities contained within an integrated system worn by a person.").

[24] Raymond & Shackelford, *supra* note 23, at 121.

[25] *See Privacy Policy*, FITBIT, http://fitbit.link/25itdKy (last visited Mar. 20, 2016) (detailing the user information Fitbit collects, including but not limited to names, email addresses, and fitness statistics).

[26] Jason Habinsky, *XpertHR Employment Law Manual 2154*, XPERTHR, http://bit.ly/1OT1KYm (last visited Feb. 1, 2016).

[27] Reg Wydeven, *Exercise Monitor Can Make a Case for Legal Claims*, POST-CRESCENT MEDIA (Nov. 30, 2014, 5:02 AM), http://post.cr/1Tvbyo1.

[28] Nicole Black, *Legal Loop: Wearable Tech Data as Evidence in the Courtroom*, THE DAILY REC. (Aug. 14, 2015), http://bit.ly/1WNYZe5.

[29] *See How it Works*, TILE, http://bit.ly/1s5rabe (last visited Jan. 24, 2016) (explaining Tile, a device that you hook to your keychain that alerts the user's phone its location through Bluetooth).

Gear,[31] and many more.[32]

B. Personal Tracking Devices on the Rise

The increased use of wearable technology, which started with the idea of health monitoring, has expanded its reach to the population as a fashion accessory.[33] Even President Obama was photographed wearing a Fitbit Surge.[34] People use these devices to monitor almost everything they can about their own bodies.[35] Professor Larry Smarr, an astrophysicist and computer scientist at the University of California at San Diego, compares the monitoring capabilities of a wearable device to the operation of a car by saying "we know exactly how much gas we have, the engine temperature, how fast we are going…[what we are] doing is creating a dashboard for [the] body."[36] Personal use of this information is very different, however, from providing a third party with all data of another person's physical activity. Transparency in someone's personal activity as a result of Fitbit data possibly violates their privacy rights as well as the Fifth Amendment right against compelled self-incrimination.

C. Fitbit Device Basics

A Fitbit monitors various bodily functions of the person wearing it; it estimates how many calories its owner burns by recording their basal metabolic rate ("BMR"), their activity recorded during the day, and those activities he or she manually enters throughout the day.[37] BMR is the "rate at which you burn

---

30 *See Vivosmart HR*, GARMIN, http://bit.ly/20s5hxG (last visited Jan. 24, 2016) (describing Garmin's wearable device that tracks fitness statistics, but can also receive texts, calls, emails, and social media alerts).

31 *See Wearable Tech*, SAMSUNG, http://bit.ly/1VfTvqF (last visited Jan. 24, 2016) (Samsung offers various wearable technology devices including viewers, trackers, and watches).

32 *See Activity Trackers & Pedometers*, BEST BUY, http://bit.ly/1TGW3Nn (last visited Jan. 24, 2016) (hundreds of different wearable technologies are available for purchase at Best Buy).

33 *See* Vikram Alexei Kansara, *Amanda Parkes on Why Wearable Tech is About More Than Gadgets*, BUS. OF FASHION (Nov. 30, 2014, 11:49 AM), http://bit.ly/1XOazVo (describing the rise of wearable technology built into clothing); *see also Tory Burch for Fitbit*, FITBIT, http://fitbit.link/22mn2Qy (last visited Jan. 24, 2016) (announcing Fitbit's partnership with fashion designer Tory Burch for luxury and high end wearable technologies).

34 Ariana Eunjung Cha, *The Revolution Will Be Digitalized,* WASH. POST (May 9, 2015), http://wapo.st/1pHIEt5.

35 *Id*.

36 *Id*.

37 *How Does Fitbit Estimate How Many Calories I've Burned?,* FITBIT, http://fitbit.link/1XOaAJ2 (last visited Jan. 24, 2016).

calories at rest just to maintain vital body functions like breathing, heartbeat, and brain activity."[38] The user's data resets every day.[39] A Fitbit also estimates the amount of steps the wearer has taken by using a three-axis accelerometer.[40] Fitbit describes the accelerometer as:

> a device that turns movement (acceleration) of a body into digital measurements (data) when attached to the body. By analyzing acceleration data, our trackers provide detailed information about frequency, duration, intensity, and patterns of movement to determine your steps taken, distance traveled, calories burned, and sleep quality. The 3-axis implementation allows the accelerometer to measure your motion in any way that you move, making its activity measurements more precise than older, single-axis pedometers.[41]

However, there have been various reports of flaws in Fitbit technology. For example, a Fitbit can register the wearer as taking several steps, when in actuality the person was just driving his vehicle.[42] While a Fitbit is not always completely accurate, Fitbit claims that adjusting the settings to a lower sensitivity level should solve most problems when it comes to activities being inaccurately recorded.[43] However, if the wearer does not have the time to constantly monitor the accuracy of a Fitbit's recordings, which most people do not, then a Fitbit's data could continue to record the inaccurate data.

Studies have shown that a Fitbit may reflect invalid data regarding someone walking on a treadmill.[44] Fitbit even admits, "Fitbit does not represent, warrant or guarantee that its trackers can deliver the accuracy or sophistication of medical devices or clinical sleep monitoring equipment."[45] Therefore, even if a Fitbit's data is found admissible in court, it is not guaranteed to be accurate or helpful.

A 2012 study evaluated a Fitbit's reliability and validity compared to widely used sleep-monitoring tests such as polysomnography and standard actigraphy.[46] While the study showed there was high intra-device reliability, it also showed the specificity of a Fitbit to correctly register and accurately identify

---

38 *Id*.

39 *Id*.

40 *How Does My Tracker Count Steps?*, FITBIT, http://fitbit.link/1TSywVK (last visited Mar. 21, 2016).

41 *Id*.

42 *Flex Counts Steps While Driving?*, REDDIT (Aug. 5, 2014), http://bit.ly/22mnkXH.

43 *How Accurate Is My Flex?*, FITBIT, http://fitbit.link/1VfThjs (last visited Mar. 21, 2016).

44 Judit Takacs et al., *Validation Of the Fitbit One Activity Monitor Device During Treadmill Walking*, 17 J. OF SCI. & MED. IN SPORTS 496, 500 (2014).

45 Jeff Zalesin, *Fitbit Buyers Step Up False Ad Claims Over Sleep-Tracking*, LAW 360 (Aug. 21, 2015, 5:24 PM), http://bit.ly/22mncHM.

46 Hawley E. Montgomery-Downs et al., *Movement Toward a Novel Activity Monitoring Device*, 16 SLEEP & BREATHING 913, 913-14 (2012) (explaining that polysomnography is the "gold standard" for sleep measurement and actigraphy as identification for sleep/wake times and patterns).

the wearer's actions was poor.[47] The study's findings were nerve-wracking to consumers since many people want to use a Fitbit to record their actual physical activity while awake.[48] Although the study admitted a Fitbit might be an adequate instrument to measure activity for the general population, it also noted a Fitbit consistently misidentified "wake as sleep and thus overestimate[d] both sleep time and quality."[49] Consequently, even admissible Fitbit data should be presented with accompanying expert testimony to help the fact finder in a court of law understand the reliability of the data recorded by a Fitbit.

D. Fitbit's Privacy Policies

Fitbit's website lists out privacy policies involved with owning a Fitbit.[50] These policies state:

> What Data May be Shared With Third Parties?
>
> First and foremost: We don't sell any data that could identify you. We only share data about you when it is necessary to provide the Fitbit Service, when the data is de-identified and aggregated, or when you direct us to share it.
>
> Data That Could Identify You
>
> Personally Identifiable Information (PII) is data that includes a personal identifier like your name, email or address, or data that could reasonably be linked back to you. We will only share this data under the following circumstances: With companies that are contractually engaged in providing us with services, such as order fulfillment, email management and credit card processing. These companies are obligated by contract to safeguard any PII they receive from us.
>
> If we believe that disclosure is reasonably necessary to comply with a law, regulation, valid legal process (e.g., subpoenas or warrants served on us), or governmental or regulatory request, to enforce or apply the Terms of Service or Terms of Sale, to protect the security or integrity of the Fitbit Service, and/or to protect the rights, property, or safety of Fitbit, its employees, users, or others. If we are going to release your data, we will do our best to provide you with notice in advance by email, unless we are prohibited by law from doing so.
>
> We may disclose or transfer your PII in connection with the sale, merger, bankruptcy, sale of assets or reorganization of our company. We will notify you if a different company will receive your PII and the promises in this Privacy Policy will apply to your data as transferred to the new entity.[51]

Fitbit's privacy policy stated above details how and when a Fitbit's data may be shared with third parties. Companies with whom Fitbit may share customer data include those contractually obligated to provide services, such as order fulfillments, in the chance that Fitbit goes bankrupt or decides to sell their

---

47 *Id.* at 913.
48 *Id.*
49 *Id.*
50 *Privacy Policy, supra* note 25.
51 *Id.* (emphasis added).

company, and circumstances in which disclosure is in connection to a legal obligation, and this data can identify the owner of the Fitbit.[52] However, the parameters of legal obligations recognized by Fitbit for this purpose are vague, and could cover nearly any legal obligation. Even more worrisome is that Fitbit is under no obligation to inform the owner that their private information has been disclosed to an outside party. Under its privacy policy, Fitbit need only to do their "best" to inform the owner.

Fitbit is relatively new to the wearable technology market, but their consumers have already faced violations of privacy through their use of a Fitbit product.[53] In 2011, an article explained how the data of several Fitbit users, who had worn their Fitbits during sexual activity, had been made available through Google search results without their consent.[54] The availability of this data may be the result of Fitbit's improper disclosures of device privacy settings, which has created a rocky relationship with some customers.

Disclosures of seemingly private data like the example above are possible because of Fitbit's default setting, which allows users' profile data to be found through various search engines.[55] In order to keep their data private, a Fitbit user has to opt out of this setting.[56] Several Fitbit users were "unwittingly sharing their most intimate details (i.e. kissing, hugging and more) when recording their sexual activity to calculate how many calories they have burned in a given period of time."[57] Some Fitbit users may want to wear their device during sex to record their 'exercise data,' but this information should not be available to the public without the wearer's express and informed consent to release it.

Naturally, Fitbit changed their policy after this scandal.[58] However, customers who purchased their Fitbit prior to this policy change are still at risk of their expectation of privacy being seriously violated.[59] As of May 2015, Fitbit's standard of privacy has been "privacy versus electronic devices, what's available for discovery and what's not, is whether you have a reasonable expectation of privacy.… That's balanced against the probative value of the data and how

---

52 *Id*.

53 Kristen Lee, *Wearable Health Technology and HIPAA: What Is and Isn't Covered*, SEARCHHEALTHIT.COM (July 2015), http://bit.ly/244S6DM.

54 Leena Rao, *Sexual Activity Tracked By Fitbit Shows Up In Google Search Results*, TECHCRUNCH (July 3, 2011), http://tcrn.ch/1NHH8SN.

55 *Id.*

56 *Id.*

57 *Id.*

58 Kashmir Hill, *Fitbit Moves Quickly After Users' Sex Stats Exposed*, FORBES (July 5, 2011, 7:58 AM) [hereinafter Hill, *Fitbit Moves Quickly*], http://onforb.es/1qFpxzs.

59 *See generally* Hunter Walker, *Senator Warns Fitbit Is a 'Privacy Nightmare' and Could Be 'Tracking' Your Movements*, BUS. INSIDER (Aug. 10, 2014, 2:20PM), http://read.bi/1s5shHV (calling for federal protections to guard consumers from a 'privacy nightmare' by Senator Chuck Schumer (D-NY) in 2014).

prejudicial it is to be the person you're getting it from."[60] The general public deserves to feel comfortable with an item on their wrist that records personal information, while also having a 'reasonable expectation of privacy' in Fitbit's information disclosure.

Presently, Fitbit's website establishes "default visibility settings," which reveal information on the use of data, and if the user wants to change who can view their user profile.[61] Even in the wake of the sexual activity scandal, privacy concerns seem to have little meaningful influence on Fitbit to change their privacy settings. [62] Nevertheless, Fitbit has attempted to improve public perception of its efforts to protect consumers' privacy.[63]

Fitbit has advertised that the company will not be selling consumer data to third parties.[64] Senator Charles Schumer (D-NY) commended Fitbit for its privacy policies in 2014 after Fitbit pledged to never sell personal identifying information ("PII") to third parties.[65] Furthermore, Senator Schumer urged the Federal Trade Commission ("FTC") to implement rules requiring companies that sell this type of fitness device to have privacy measures on the data gathered from consumers.[66]

In light of the rise in the use of wearable technology by everyday people, it is imperative for lawyers to know how this technology will affect the discovery process in the judicial system.[67] Similarly, the Federal Rules of Evidence and its comments will need to be adjusted to keep up with what is defined as discoverable.[68] Perhaps over the next decade or so, sufficient case law will be established to guide courts on how wearable technology may be used as credible and reliable evidence.[69] To get a head start on new, emerging technology, any

---

60 Amanda Crosswhite, *Wearables: E-discovery's New Frontier?*, R.I. LAWYERS WEEKLY (May 14, 2015), http://bit.ly/27QS1YS.

61 *Let's Talk about Privacy, Publicly*, FITBIT, http://fitbit.link/1VfTmUi (last visited Mar. 16, 2016).

62 Dana Liebelson, *Are Fitbit, Nike, and Garmin Planning to Sell Your Personal Fitness Data?*, MOTHER JONES (Jan. 31, 2014, 7:00AM), http://bit.ly/25cmYoj.

63 *See* Laura Ryan, *Fitbit Hires Lobbyists After Privacy Controversy,* NAT'L J., (Sept. 15, 2014), http://bit.ly/1Wdz3I8 (finding Fitbit changed its policies to respond to privacy concerns).

64 *Id*.

65 Lance Duroni, *Fitbit Doing 'Right Thing' With Privacy Policy, Schumer Says*., LAW 360 (Aug. 25, 2014, 2:36 PM), http://bit.ly/1sydQvZ.

66 *Id.*

67 MODEL RULES OF PROF'L CONDUCT r 1.1 (AM. BAR ASS'N 2013) ("A lawyer shall provide competent representation to a client. Competent representation requires the legal knowledge, skill, thoroughness, and preparation reasonably necessary for the representation.")

68 *See generally* FED. R. EVID. The Federal Rules of Evidence does not discuss what is deemed and what is not deemed discoverable. *Id.*

69 Sarah Griffiths, *Fitbit Data is Now Being Used in COURT: Wearable Technology is*

rules and guidelines must be broad enough to cover analogous technology.

E. Fitbit: A Possible Medical Device

Fitbit is classified as a "wrist-worn [wearable]," which is "worn on the person for use in varied applications from health to finance."[70] A Fitbit's health monitoring aspect is important because it replicates the "sensor capabilities of medical devices worn close to the skin."[71] Fitbit's website acknowledges, "Fitbit designs products and tools that track everyday health and fitness to empower and inspire users to lead healthier, more active lives."[72] When dealing with a miniature portable medical devices, the Food and Drug Administration ("FDA") "requires mobile medical app developers to create a cyber security plan and submit it to the FDA.… But this only applies to mobile medical apps and not to wearable health technology generally."[73] Therefore, FDA regulations do not currently apply to wearable technology. However, considering many Fitbit devices are recommended by physicians,[74] Fitbits could broadly be considered a form of a medical application and ought to fall under FDA's purview and be subject to its regulations.[75]

F. Fitbit's Possible Medical Confidentiality Violations

The Health Insurance Portability and Accountability Act ("HIPPA") Privacy Rule was passed by Congress to

> …establish national standards to protect individuals' medical records and other personal health information and applies to health plans, health care clearinghouses, and those health care providers that conduct certain health care transactions electronically. The Rule requires appropriate safeguards to protect the privacy of personal health information, and sets limits and conditions on the uses and disclosures that may be made of such information without patient authorization. The Rule also gives patients rights over their health information, including rights to examine and obtain a copy of their health records, and to request corrections.[76]

However, thus far the HIPPA Privacy Rule has not been applied to most in-

---

Set to Revolutionise Personal Injury and Accident Claims, DAILYMAIL (Nov. 17, 2014, 11:56 PM), http://dailym.ai/25cnEtG.

70 Raymond & Shackelford, *supra* note 23, at 121-22.

71 *Id.* at 122.

72 *Privacy Policy*, *supra* note 25.

73 Karen H. Bromberg & Duance C. Cranston, *Wearable Technology: Taking Privacy Issues to Heart*, N.Y.L.J., 1, 2 (Mar. 2, 2015).

74 Ken Terry, *A Physician's Guide to Prescribing Mobile Health Apps,* MED. ECON. (Oct. 8, 2014), http://bit.ly/244SMJp.

75 Colin Lecher, *The FDA Doesn't Want to Regulate Wearables and Device Makers Want to Keep It That Way*, THE VERGE (June 24, 2015, 2:07PM), http://bit.ly/244T7vx.

76 *The HIPAA Privacy Rule*, DEPT. OF HEALTH & HUMAN SERV. http://1.usa.gov/1pqlYgX (last visited Mar. 20, 2016).

formation obtained by wearable technology because companies, such as Fitbit, are not bound by the same confidentiality requirements as a physician. Therefore, the data could "theoretically be made available for sale to marketers, release under subpoena in legal cases with fewer constraints."[77] The data not covered by this act was an issue raised in 2014 by Federal Trade Commission Commissioner Julie Brill, who acknowledged:

> … although consumers can gain significant benefits from new medical services such as devices that measure physical activity, she was concerned about letting the data linger outside the protections afforded to other types of medical data that is provided directly to physicians and other entities that are covered by the Health Insurance Portability and Accountability Act.[78]

Hence, the possibility of this type of information should be a concern because it is not protected in the same manner as medical data and therefore, should be treated as a potential health law and privacy concern. This issue was addressed in a recent article by *The New York Law Journal*:

> [The] debut of the Apple Watch in fall 2014 may mark a watershed moment not only in the technology industry, but also in the areas of privacy and health law. The technology embedded in the watch-and in competing devices, such as Fitbit and Jawbone-effectively shifts health care from the physical to the remote, and in the process creates a mechanism for the online collection of highly sensitive health information.[79]

However, HIPPA has yet to regulate Fitbits, perhaps because the law views the wearable devices as merely a technology fad.[80] Nevertheless, new issues arise as more employers are purchasing Fitbits as a means of monitoring of their employee's health.[81]

G. Fitbits Purchased by Employers

Employer's legal access to their employees' Fitbits is an important issue since it is becoming more common practice for employers to purchase Fitbits for their employees as "part of an employer-sponsored wellness plan to monitor health and fitness."[82] Benefits to one employer's wellness plan include "enhanced work communications, increased workplace safety and aid in monitoring employee conduct, productivity and employee training."[83] There are possi-

---

77 Ariana Eunjung Cha, *Wearable Gadgets Portend Vast Health, Research and Privacy Consequences,* WASH. POST (May 17, 2015) [hereinafter Cha, *Wearable Gadgets*], http://wapo.st/1pHIEt5.

78 Duroni, *supra* note 65.

79 Bromberg & Cranston, *supra* note 73, at 1.

80 Lee, *supra* note 53, at 2.

81 Jay Hancock, *Workplace Wellness Programs Put Employee Privacy at Risk*, CNN (Oct. 2, 2015, 12:37PM), http://cnn.it/1WL4GbZ.

82 Habinsky*, supra* note 26.

83 *Id.*

ble drawbacks—including "access to inappropriate information, loss of employee productivity, and concentration, harassment and privacy issues, as well as safety hazards and the potential disclosure of the employer's confidential information."[84] Furthermore, if a Fitbit is not purchased for personal use but instead by a wearer's employer, could this affect the privacy of the information recorded on the wearer's Fitbit?

It has been established that if a wearer or an employee is wearing an employer-owned Fitbit then the wearer has lost his or her privacy rights with this device.[85] Although technology has reduced certain expectations of privacy throughout the years, "employees still expect employers to respect personal privacy."[86] In the *Risley* case, the expectation of privacy could become an issue if the alleged victim's employer purchased her Fitbit and thus the data is at the employer's disposal. If the alleged victim of a crime is also an employee trying to establish her boss sexually assaulted her, could her employer reasonably prevent the release of the Fitbit's data as evidence against him?

H. Use of a Fitbit in Litigation

In 2014, a Canadian law firm represented a young woman who was hurt in an accident.[87] To demonstrate the extent of her injuries, the young woman's lawyers used her Fitbit to measure her activity levels after the accident.[88] The plaintiff's lawyers planned to use physical activity data from their client's Fitbit tracker at trial to show how her lifestyle had been severely impacted by her injuries.[89] The results showed that because of her accident, her activity level was less than that of an average woman of her age and profession.[90] This is the first case seen where a plaintiff's lawyer was able to use the physical activity data from their client's Fitbit tracker at trial to show the impact on one's lifestyle resulting from injuries at issue.[91] Therefore, it could be advantageous to consider using a Fitbit to assist in personal injuries cases, when the harmed party chooses to do so.

However, there is a vast difference between the use of a Fitbit in the aforementioned case with that of the *Risley* case. While a Fitbit assisted in finding justice in this personal injury case, the use of Fitbit data to reveal personal be-

---

84 *Id.*
85 Lee*, supra* note 53, at 2.
86 Habinsky*, supra* note 26.
87 Parmy Olson, *Fitbit Data Now Being Used In The Courtroom,* FORBES (Nov. 16, 2014, 4:10 PM), http://onforb.es/1TSzwJJ.
88 *Id*.
89 Crosswhite, *supra* note 60.
90 Wydeven, *supra* note 27.
91 Crosswhite, *supra* note 60.

haviors could negatively impact a rape victim's willingness to report their attack, and add to the high number of unreported rapes.[92] Furthermore, it fuels the victim blaming unfortunately frequently involved with victims of rape.

In a case in San Francisco involving a wearable device, attorneys obtained data from a wearable technology, called Strava, to show the defendant had been speeding and was responsible for the accident in controversy.[93] Strava, a competitor of Fitbit, tracks a person's runs, rides, and cross-training and can also be uploaded to the person's phone to log all of their workouts.[94] This technology will be influential in the future. According to Vincent L. Green, President of the Rhode Island Association for Justice, "[f]ive years from now, it will be commonplace for lawyers to be asking questions about what kind of data do you have running on your Apple watch."[95]

III. CONSIDERING THE REPERCUSSIONS OF INVESTIGATING FALSE RAPE ALLEGATIONS THROUGH VICTIMS' FITBITS

A. The Legal Foundation

In *Riley v. California*, during an oral argument in the Supreme Court of the United States, the petitioner stated that Fitbits tell the Court the same information that they were worried about in *United States v. Kyllo*; further, these devices monitor not only the home but also the inside of people's bodies.[96] In *Kyllo*, the Supreme Court was concerned with the violation of privacy rights in the police-use of technology to survey someone's private property.[97] In *Kyllo,*

---

92 *Reporting of Sexual Violence Incidents*, NAT'L INST. OF JUSTICE (Oct. 26, 2010), http://bit.ly/25iuDEQ ("Only 36 percent of rapes, 34 percent of attempted rapes, and 26 percent of sexual assaults were reported.")

93 John G. Browning, *Legally Speaking: When All Else Fails, Blame Social Media,* SE. TEX. REC. (July 6, 2012, 8:37 AM), http://bit.ly/25iuilK.

94 *Strava Features*, STRAVA, http://bit.ly/1OT2JYD (last visited Jan. 23, 2016) (finding that a tracking device of your activities that can be uploaded online, it comes in the form of a chip, bracelet, dongle, etc.).

95 Crosswhite, *supra* note 60.

96 Transcript of Oral Argument, *supra* note 18, at 18. Riley was stopped for expired vehicle registration tags, at which point an officer discovered two handguns under the hood of the car. With the guns and gang paraphernalia found during the traffic stop, Riley was arrested and the police searched his cell phone without a warrant. These guns were linked to a gang murder for which Riley was a suspect, and police subsequently were able to charge Riley for his connecting in the shooting based on pictures and videos found on the phone. The Court ruled that the police cannot search digital information on a cell phone without a warrant, and is very different than physical things or information, as digital information cannot harm the arresting officer or make it possible for the arrestee to escape. *Id.*

97 Upon reasonable suspicions that the Defendant was growing marijuana in his house,

the court established that a Fourth Amendment search[98] does not occur unless "the individual manifested a subjective expectation of privacy in the object of the challenged search," and "society [is] willing to recognize that expectation as reasonable."[99]

B. Commonwealth of Pennsylvania v. Jeannine Risley: The Basis for this Scenario

In March 2015, a disgruntled employee, Jeannine Risley from St. Petersburg, Florida, claimed that an intruder had raped her in her sleep.[100] During the night of the incident, Ms. Risley was staying at her boss' home in Pennsylvania.[101] That night, "police were called to the home where they found overturned furniture, a knife and a bottle of vodka."[102] When police arrived Ms. Risley told them "an unknown man pulled her out of bed, attacked her in a bathroom and raped her at knifepoint."[103] She also stated "she'd been sleeping and that she was woken up around midnight and sexually assaulted by a 'man in his 30s, wearing boots.'"[104]

Her Fitbit then became a witness against her.[105] At first, Ms. Risley claimed she had been wearing her Fitbit band at the time of the attack.[106] She then claimed that her Fitbit had been lost during the assault.[107] The police found it in the hallway a few feet away from the bathroom.[108] When the police examined her Fitbit, the data retrieved from the device indicated that she may have been

---

police used thermal-imaging from outside of the defendant's house which detected heat. The police used this information from the device to get a search warrant which resulted in the defendant's arrest. The Court ruled that it is a Fourth Amendment search if the police get information from a home without physical intrusion by using a device that would not normally be used by the public, and thus requires a warrant. Kyllo v. United States, 533 U.S. 27, 33 (2001).

98 *What Does the Fourth Amendment Mean?*, U.S. CTS., http://1.usa.gov/1TSznWE (last visited Jan. 23, 2016).

99 *Kyllo*, 533 U.S. at 33 (citing California v. Ciraolo, 476 U.S. 207, 213 (1986)).

100 Kevin Chase, *Stupid Criminals: Fitbit Contradicts a Woman's Sexual Assault Allegations*, KBAT 99.9 (June 23, 2015, 2:28 PM), http://bit.ly/1TzsQ5R.

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

102 Kashmir Hill, *Fitbit Data Just Undermined a Woman's Rape Claim*, FUSION (June 25, 2015, 1:57 PM) [hereinafter Hill, *Fitbit Data*], http://fus.in/1TSA0zi.

103 Myles Snyder, *Police: Woman's Fitness Watch Disproved Rape Report*, ABC NEWS (July 19, 2015, 2:03PM) http://bit.ly/1RldnSh.

104 Brett Hambright, *Woman Staged 'rape' Scene with Knife, Vodka, Called 9-1-1, Police say,* LANCASTERONLINE (June 19, 2015), http://bit.ly/1RK7Vcv.

105 Hill, *Fitbit Data, supra* note 102.

106 *Id.*

107 *See* Kleeman*, supra* note 101.

108 *Id.*

walking around at the time of the alleged attack.[109] The police claimed that Ms. Risley gave them the password to access her Fitbit, as well as consent to search and collect the stored data within it.[110] The criminal complaint against Ms. Risley was for perjury, and stated that a Fitbit proves that Ms. Risley had lied because it shows that she "had been awake and walking around the entire night, not sleeping as she had claimed."[111]

However, more facts will be necessary to determine if Ms. Risley consented to the police search of her Fitbit. As seen in *Riley v. California*, the Supreme Court does not allow the search of digital information on a smart phone incident to arrest without a warrant.[112] Since Ms. Risley was the alleged victim and not the one being arrested in this case, much more information will have to be ascertained regarding the facts of that night.[113] 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.[114] 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 period of time.[115] 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. As a result, a stricter set of rules is needed in order to allow data from wearable technology to be introduced as evidence.[116]

In *Risley*, the police also found no evidence of an intruder, such as footprints or tracks, in the snow just outside the home.[117] Documents filed with the Pennsylvania court reveal that her boss, whom has yet to be named,[118] told Ms. Risley that she was going to lose her role as a temporary director with the compa-

---

109 Hambright, *supra* note 104.

110 Le Trinh, *Can Your Fitbit Data Be Used Against You in Court?*, FINDLAW: BLOGS (July 14, 2015, 2:59 PM), http://bit.ly/1VfU9EI.

111 *See* Snyder*, supra* note 103.

112 *Riley*, 573 U.S. ___, 134 S. Ct. at 2493.

113 SEAN E. GOODISON, ROBERT C. DAVIS & BRIAN A. JACKSON, NAT'L CRIM. JUST. REFERENCE SERV., 2013-MU-CX-K003, DIGITAL EVIDENCE AND THE U.S. CRIMINAL JUSTICE SYSTEM 7 (2015), http://1.usa.gov/1s5tnDq.

114 Treacher, *supra* note 19.

115 *Compare* Nathan Chandler, *How FitBit Works*, HOWSTUFFWORKS: TECH (May 2, 2012), http://bit.ly/1U7ehn3 (detailing the process of recording the steps you take, calories burned, and sleep patterns) *with* United States v. Jones, 565 U.S. ___, 132 S. Ct. 945, 955-57 (2012) (Sotomayor, J., concurring) (explaining law enforcement's use of an aggregated sum of an individual's movements obtained through GPS and other location tracking technologies paint a mosaic of the intricate and private details of an individual's life).

116 Alexander Howard, *How Data From Wearable Tech Can Be Used Against You In A Court of Law*, HUFFINGTON POST (June 30, 2015), http://huff.to/1s5tzT5.

117 Hill*, Fitbit Data*, *supra* note 102.

118 *See id.*

ny.[119] Ms. Risley "was charged with false reports to law enforcement, false alarms to public safety, and tampering with evidence."[120] A trial date is set for later this year unless she chooses to enter a plea.[121]

The complaint was filed against Ms. Risley by the Commonwealth of Pennsylvania on June 30, 2015 and claimed three charges against her for the March 10, 2015 occurrence: false alarm to agency of public safety, tampering with or fabricating physical evidence, and false reports-reported offense did not occur.[122] As of June 2015, Ms. Risley and her defense attorney have waived a preliminary hearing on all counts, which does not admit her guilt, but does concede that there is some evidence to support the charges.[123] In response, the Magistrate District Judge ordered Ms. Risley to be tried in Lancaster County Court of Common Pleas.[124] "Ms. Risley appeared at the hearing with her husband and … said very little to [the] Judge."[125] She was "allowed to remain free on unsecured bails until her next hearing."[126]

C. The Pennsylvania State Prosecutors – Next Steps Available

The Court of Common Pleas ought to dismiss the case and the alleged victim should not face any legal repercussions because trying it will do more harm then good for society as a whole. The potential for victim-blaming in this case misleadingly highlights the minimal amount of false rape claims that there are in comparison to valid rape claims.[127] Fact finding will be particularly essential in this case, because the evidence the police found outside the home should not be sufficient to prove that Ms. Risley made up the entire incident.[128] Furthermore, the fact that her story had changed, regarding the whereabouts of her Fitbit, should not be a sufficient basis to claim that she is lying, since it is not uncommon for someone that would have just suffered an attack on his or her person to be confused.[129] Additionally, the psychological trauma involved with a rape can seriously affect the rape victim's recollection of the incident.[130] It

---

119 *See id*.
120 Snyder, *supra* note 103.
121 *See* Hambright*, supra* note 104.
122 Commonwealth v. Risley, Criminal Docket: CP-36-CR-0002937-2015 (Lancaster County, Pa., initiated Apr. 14, 2015).
123 *See* Hambright*, supra* note 104.
124 *Id.*
125 *Id.*
126 *Id.*
127 *See* Kleeman*, supra* note 101.
128 *See generally* Hambright*, supra* note 104 (recognizing the lack of evidence enumerated in the article and police report).
129 *See* Hill*, Fitbit Data*, *supra* note 102.
130 *Tinsley*, 895 F.2d at 524.

would be absurd to expect that a rape victim's focus would be on the location of his or her Fitbit during an attack. And most importantly, this case raises several concerns of law enforcement protocols regarding sexual assault to victims.

D. Ms. Risley's Fitbit—Implications & Admissibility

Ms. Risley first told the police that she had been wearing her Fitbit during the attack and then changed her story to that she had lost it during the attack.[131] However, it is hard to claim that any rape victim would be thinking about the whereabouts of their Fitbit during such a traumatic experience. This part of her testimony has not been questioned in any of the news articles thus far, but it should be thoroughly examined when and if this case goes to trial. [132] The incident happened in Pennsylvania where the state law on evidence declares:

Admissibility of evidence is a matter addressed to the sound discretion of the trial court, which may only be reversed upon a showing that the court abused its discretion. Pennsylvania recognizes a state of mind hearsay exception because determining one's state of mind is often impossible without such statements and such statements are presumed reliable because of their spontaneity. However, state of mind evidence must still meet the test of relevance. Determination of the relevancy of evidence offered at trial requires a two-step analysis. It must be determined first if the inference sought to be raised by the evidence bears upon a matter in issue in the case and, second, whether the evidence renders the desired inference more probative than it would be without the evidence.[133]

While Ms. Risley's statements regarding the whereabouts of her Fitbit were made with spontaneity, a strong and compelling argument should be made that her state of mind at the time was compromised due to the trauma she had just experienced. The Fitbit data was deemed to be relevant to the rape investigation once the police had a chance to go through it, but the Commonwealth should have to prove the relevance of the evidence of asking for a Fitbit from a rape victim during their initial visit to the scene.

Pennsylvania courts have established that to obtain a warrant for the Fitbit and its data, the judge or magistrate must be able to decide that "given all of the circumstances set forth … there is a fair probability that contraband or evidence of a crime will be found in a particular place."[134] The issue has become whether Ms. Risley was actually attacked. The state court should not consider

---

131 *See* Hill, *Fitbit Data*, *supra* note 102.
132 *Tinsley*, 895 F.2d at 524.
133 Commonwealth v. Hawkins, 701 A.2d 492, 507 (Pa. 1997).
134 *Id*.

the Fitbit data in regards to the issue in this case until they have a clear sense of the facts of that night. For instance, if Ms. Risley truly did lose the Fitbit during the attack, then its possible that the attacker had it on his person. Therefore, the movements recorded by the Fitbit were not those of Ms. Risley, but those of the attacker.

Secondly, the court will have to evaluate "whether the evidence renders the desired inference more probative than it would be without the evidence."[135] For this part of the test, more facts will need to be presented to the court to show that there is no other source of evidence that could present what the Fitbit's evidence shows.[136] However, it will be hard for the Fitbit evidence to be considered probative, unless it can first be established that Ms. Risley was in fact wearing a Fitbit during the time of the attack, since a Fitbit records data but cannot identify specific actions nor whose movements it is recording.[137] Therefore, the movements the Fitbit recorded could have easily been the assailant's.

E. Pursuing a False Rape Accusation

When this case goes to trial and if Ms. Risley does not accept a plea bargain, the prosecution will attempt to prove that Ms. Risley's rape allegations were false. This could allow the prosecution to admit into evidence prior false rape accusations that she has committed, if any.[138] While permissible, the court should think twice about the policy implications as it will strengthen the possibility of future victim-blaming in similar cases. Other states have held differently. Ohio courts, for instance, have held that:

If the trial court determines that rape accusations previously made by a witness were entirely false (that is, that no sexual activity had been involved) the trial court would then be permitted to exercise its discretion in determining whether to permit defense counsel to proceed with cross-examination of the alleged victim. Where an alleged rape victim admits on cross-examination that she has made a prior false rape accusation, the trial judge shall conduct an in camera hearing to ascertain whether sexual activity was involved and, as a result, would be prohibited by Ohio Rev. Code Ann. § 2907.02(D), or whether the accusation was totally unfounded and therefore could be inquired into on cross-examination pursuant to Ohio R. Evid. 608(B).[139]

Therefore, under the analysis of the Ohio court applied to these facts, in or-

---

135 *Id.* at 507.

136 *See id.* (illustrating that the Fitbit would, as in Commonwealth v. Hawkins, render the inference more probative than without the Fitbit).

137 *Sleep Tracking FAQs*, FITBIT, http://fitbit.link/1XOdJbG (last visited Jan. 24, 2016).

138 FED. R. EVID. 404(b).

139 State v. Boggs, 588 N.E.2d 813, 817 (Ohio 1992).

der for previous false rape allegations to be admissible, there would still be a good amount of fact finding that will have to be done. Due to the limited facts reported about this case, it is unknown whether there was any evidence of sexual activity besides Ms. Risley's statement to the police.[140]

IV. AMBIGUITY OF CURRENT ELECTRONIC EVIDENCE POLICIES

A. Legal framework

The legal framework of wearable technology as admissible evidence needs to adapt quickly to keep up with ever changing technology. Even the Supreme Court of the United States has acknowledged the need to develop this area of law. Chief Justice Roberts posed the question of what data can be examined from a Fitbit during oral arguments in a 2014 case:

> [w]hat if you have a device that doesn't have the broad information that a smartphone has, but only a very limited, like a Fitbit that tells you how many steps you've taken, and the defendant says, I've been in my house all afternoon, and they want to check and see if he's walked 4 miles. It's not his whole life, which is a big part of your objection. Is that something they can look at?[141]

The FDA has also taken note that "[i]nnovation is outpacing the scientific and legal framework for testing and regulating such devices. In January 2015, the Food and Drug Administration indicated it would regulate devices that are invasive but take a lighter touch on wearables." [142] Since a Fitbit is considered a low-risk, general wellness product, under the current regime, it is free from extra scrutiny under federal food and drug safety laws. [143] However, Fitbits are now being used to disprove criminal claims. Therefore, labeling this product as low-risk is clearly an understatement.

In the 2014 case of *Riley v. California*, the Supreme Court of the United States held the "(1) interest in protecting officers' safety did not justify dispensing with warrant requirement for searches of cellphone data, and (2) interest in preventing destruction of evidence did not justify dispensing with warrant requirement for searches of cell phone data."[144] Based on this case law from the highest court in the country, a Fitbit's data cannot simply be downloaded without a warrant or consent.[145] There is no fathomable argument a po-

---

[143] Dustin Volz, *Here's What Happens When the Supreme Court Talks About Cell Phones for Two Hours,* THE NAT'L J. (Apr. 29, 2014), http://bit.ly/1NHIE7t.

[141] Transcript of Oral Argument, *supra* note 18, at 15.

[142] Cha, *Wearable Gadgets*, *supra* note 77.

[143] *Id*.

[144] *Riley*, 573 U.S. ___, 134 S. Ct. at 2474.

[145] *See* Andrew Pincus, *Evolving Technology and the Fourth amendment: The Implica-*

lice officer can make to say they must check a Fitbit to confirm that they are not in danger; especially since a Fitbit cannot store or do the diverse amount of things a cell phone can it would be hard, if not impossible, to argue that the officer needed to get into the Fitbit and check the data for his or her safety. [146]

B. Defining Digital Evidence and Explaining How It is Created and Stored[147]

The admissibility of digital evidence in court is still a rather new topic.[148] The question of when digital evidence will be admissible is rooted in the difference between digital information and physical items.[149] While "[p]hysical items at the scene can pose a safety threat and have destruction possibilities that aren't present with digital evidence … once you get in the digital works, you have the framers' concern of general warrants and the—writ of assistance."[150] The digital information argument has already been made in the context of information stored on smart phones.[151] The information on one's cellphone is private and should not to be shared with anyone, unless the smart phone owner chooses to do so based on express consent.[152] Trying to argue that the police can search specific applications, such as Facebook, because they "don't have an air of privacy about them"[153] is not legally sound.[154]

Digital evidence may be obtained from "any piece of technology that processes information" that could be "used in a criminal way."[155] At its core, "information that is stored electronically is said to be 'digital' because it has been broken down into digits; binary units of ones (1) and zeros (0), that are saved

---

tions of Riley v. California, 13 CATO S. CT. REV. 307, 329 n.86 (2014).

> "Information-collecting sensors—one example is the increasingly ubiquitous "Fitbit" device that monitors an individual's movements and could, for example, record data indicating that the wearer was likely involved in a physical altercation—should fall within the same category. Government prosecutors might try to argue that sensors collecting a single category of information should not be encompassed under *Riley*'s rationale, but the comprehensive nature of that information, and the fact that it previously has been unavailable to government agents, fit well within *Riley*, as well as the approach taken by *Kyllo* and the *Jones* concurrences."

146 *See Riley*, 573 U.S. ___, 134 S.Ct. at 2494.

147 LARRY E. DANIEL & LARS E. DANIEL, DIGITAL FORENSICS FOR LEGAL PROFESSIONALS: UNDERSTANDING DIGITAL EVIDENCE FROM THE WARRANT TO THE COURTROOM 4-9 (2012).

148 SHIRA A. SCHEINDLIN & DANIEL J. CAPRA, ELECTRONIC DISCOVERY AND DIGITAL EVIDENCE IN A NUTSHELL 287-308 (2009).

149 Transcript of Oral Argument, *supra* note 18, at 8.

150 *Id.*

151 *Id*. at 7.

152 *Id*. at 10-11.

153 *Id.*

154 *Id.*

155 NAT'L FORENSIC SCI. TECH. CTR., A SIMPLIFIED GUIDE TO DIGITAL EVIDENCE 1 (2009) [hereinafter A SIMPLIFIED GUIDE TO DIGITAL EVIDENCE], http://bit.ly/1NHIpsT.

and retrieved using a set of instructions called software or code."[156] It includes "information and data of value to an investigation that is stored on, received or transmitted by an electronic device."[157] This raises the question as to whether a Fitbit's data would be considered digital evidence since a Fitbit use this same binary language to transmit information.[158]

Digital evidence is divided into three categories: internet-based, stand-alone computers or devices, or mobile devices.[159] Considering the broad definition assigned to digital evidence, it would be hard to make an argument that a Fitbit's data does not fall within that definition of digital evidence. Nonetheless, it would be hard to designate which specific category a Fitbit or other similar wearable technology would fall under. Fitbits "connect to the internet or a user's computer or smartphone, and, in conjunction with an application or website, allow the user to view and analyze the date collected, set or track fitness goals, and collect other information relevant to the user's health and fitness plans."[160] Most Fitbits sync to the Fitbit owner's computer via a dongle—a wireless USB transmitter, or a mobile phone's Bluetooth[161] it could be possible to argue that a Fitbit's capabilities amount to a stand-alone computer or device because they do not technically require the assistance of any other computer to perform its functions.[162] A Fitbit would most likely be categorized as a database that is essentially a "list of information that a person or entity would want to maintain."[163]

C. Wearable Technology to Fall Under Mobile Device Category?

Congress has defined a mobile device as "a device that—(A) is designed to be carried on the person of the user or to be reasonably portable; (B) provides computing and communications functionality; and (C) is capable of providing access to commercial mobile service or commercial mobile data service."[164] A

---

156 *Id.*

157 NAT'L INST. OF JUSTICE, NCJ 219941, ELECTRONIC CRIME SCENE INVESTIGATION: A GUIDE FOR FIRST RESPONDERS, at ix (2008), http://1.usa.gov/27QRqq4.

158 Sean Greene, *Electronic Evidence Expert Witness: Will Fitbit and Crowdsourcing Change Personal Injury Cases?,* EVIDENCE SOLUTIONS, INC., http://bit.ly/27QROFf (last visited Mar. 22, 2016).

159 A SIMPLIFIED GUIDE TO DIGITAL EVIDENCE, *supra* note 155, at 1.

160 *Fitbug Ltd.*, 78 F.Supp.3d at1184.

161 Vincent Nguyen, *Fitbit Flex Review*, SLASH GEAR (May 6, 2013), http://bit.ly/1RlevFo.

162 *See generally* Lisa Eadicicco, *This Futuristic Armband Lets You Control Your Computer Like Magic,* TIME (Jan. 20, 2016, 11:58 AM), http://ti.me/1WdBeeH.

163 *See* DANIEL & DANIEL, *supra* note 147, at 288.

164 H.R. 1999 § 343, 114th Cong. (2015).

Fitbit is designed to be carried on the user, but because it is not a source of communication or capable of providing access to "commercial mobile data service" it would not fall under the mobile device category.[165] The case law on how courts have applied the rules of evidence to mobile devices most likely align with the path for how courts should rule on the admissibility of Fitbits and other wearable technology. Therefore, digital evidence seems to be the most accurate category applicable to Fitbits and other wearable technology.

D. Accompanying Expert Testimony

When dealing with types of technology that the general public does not thoroughly comprehend, expert testimony is "likely to hold 'unique weight' in the mind of a jury."[166] Future litigation would be greatly benefitted by mandating expert testimony when a Fitbit, or other wearable technology, has been found admissible through a warrant or other Fourth Amendment remedy.[167] Courts have consistently held that expert testimony "usurp[s] either the role of the trial judge in instructing the jury as to the applicable law or the role of the jury in applying that law to the facts before it."[168] Expert testimony is subject to the Federal Rules of Evidence 702[169] and 403[170] and "may be excluded if its probative value is substantially outweighed by the danger of unfair prejudice, confusion of the issues, or misleading the jury."[171] Therefore, when data from wearable technology is found to be admissible legal evidence through a warrant or other Fourth Amendment remedy, the trier of fact would greatly benefit from mandated expert testimony to explain the accuracy and details of the data recorded by the wearable technology.

One of the challenges to consider when dealing with permissible Fitbit evidence is whether "expert testimony [should] be required to explain how search protocols were constructed."[172] The use of technology experts as witnesses for review by the court system would be the first step in moving forward because

---

165 H.R. 1999 § 343, 114th Cong. (2015).

166 Green Mt. Chrysler Plymouth Dodge Jeep v. Crombie, 508 F.Supp.2d 295, 312 (D.Vt. 2007).

167 Justin P. Murphy & Louisa K. Marion*, Digital Privacy and E-Discovery in Government Investigations and Criminal Litigation, in* THE STATE OF CRIMINAL JUSTICE 2015, at 95, 119 (2015), http://bit.ly/1TztpfW.

168 United States v. Bilzerian, 926 F.2d 1285, 1294 (2d Cir. 1991).

169 FED. R. EVID. 702 (listing the qualifications for an expert witness's testimony).

170 FED. R. EVID. 403 ("The court may exclude relevant evidence if its probative value is substantially outweighed by a danger of one or more of the following: unfair prejudice, confusing the issues, misleading the jury, undue delay, wasting time, or needlessly presenting cumulative evidence.")

171 Nimely v. City of New York, 414 F.3d 381, 397 (2d Cir. 2005) (quoting FED. R. EVID. 403).

172 SCHEINDLIN & CAPRA, *supra* note 148, at 144.

it would allow the judge and the jury to have a better understanding of the evidence they would be presented with and the basic information on how the technology in question operates.[173] One of the challenges to consider when dealing with permissible Fitbit evidence is whether "expert testimony [should] be required to explain how search protocols were constructed."[174] The use of technology experts as witnesses for review by the court system would be a great first step in moving forward because it would allow the judge and the jury to have a better understanding of the evidence they would be presented with and the basic information on how the technology in question operates.[175] There is already case law and federal rules regarding the admissibility of expert testimony on relevant evidence.[176] Under the Federal Rules of Evidence, relevant evidence is when "(a) it has any tendency to a fact more or less probable than it would be without the evidence; and (b) the fact is of consequence in determining the action."[177] "[The] basic standard of relevance thus is a liberal one."[178]

The Supreme Court held in *Daubert v. Merrell Dow Pharmaceuticals, Inc.,* that admissibility of scientific expert testimony is admissible only if it is both relevant and reliable.[179] *Daubert* also established that the trial judge has a "gatekeeping" obligation that is not only based on scientific knowledge, but also on testimony based on technical and other specialized knowledge.[180] If expert testimony were to be introduced regarding Fitbit data, the expert would have to provide relevant and reliable information regarding that Fitbit data to meet this standard. Furthermore, it would be up to the judge's discretion to decide if the expert testimony is based on scientific, technical, or specialized knowledge.[181]

The Federal Rules of Evidence allow for testimony by an expert witness as long as he or she is "qualified by knowledge, skill, experience, training, or education" or he or she,

> may testify in the form of an opinion or otherwise if: (a) the expert's scientific, technical, or other specialized knowledge will help the trier of fact to understand the evidence or to determine a fact in issue; (b) the testimony is based on sufficient facts or data; (c) the testimony is the product of reliable principles and methods; and (d) the

---

173 *Id*. at 153.
174 *See id*. at 144.
175 *See id*. at 153.
176 *See* Daubert v. Merrell Dow Pharms. Inc*.,* 509 U.S. 579, 595 (1993); FED. R. EVID. 702.
177 FED. R. EVID. 401.
178 *Daubert*, 509 U.S. at 587.
179 *Id.*
180 *Id.* at 597.
181 *Id.*

expert has reliably applied the principles and methods to the facts of the case.[182]

A basic understanding of Fitbit data, and how such data is collected and stored, will allow the trier of fact to make a more educated decision on whether the data acquired from a Fitbit helps to prove that something either did or did not happen. Having a neutral expert would be ideal because it would allow valid information to be introduced as evidence without bias by either side.[183] In such a scenario, both sides could argue for their positions by direct and cross-examination of the expert witness.[184] However, it must first be considered whether this data is admissible.[185] Once it has been decided that the defendants have access to the data, then the Federal Rules of Evidence will apply. Therefore, the Federal Rules of Civil Procedure ("FRCP") must be discussed to understand what information will be discoverable when dealing with litigation.

E. Not Reasonably Accessible Data – Rule 26(b)(2)(B)[186]

While the issue at hand is criminal, the admissibility of wearable technology in civil cases will also likely be a legal problem in the near future. The FRCP states that the production of electronically stored information allows an objection to the request if no form was specified or the party did not state the intended use.[187] Therefore, if Fitbit's electronically stored information about a person is requested from opposing counsel, they would have to specify the reason for why they need the data or what they intend to do with it.[188] They should not be able to demand that someone disclose this private information in the hopes of finding something that will contradict the Fitbit owner's story or testimony.[189]

FRCP Title V Section E discusses that the production of electronically stored information must be done through the documents type specified in the request.[190] If no form is requested, then it must be done in the form the information is "ordinarily maintained."[191] Electronically stored information does not

---

182 FED. R EVID. 702.

183 *Cf.* FED. R. EVID. 702 (explaining that the current Federal Rules of Evidence lack a neutrality requirement for expert witness testimony).

184 *See* FED. R. EVID. 611 (detailing the rule governing the mode and order or interrogating witnesses and limiting the scope of cross-examination).

185 *See* FED. R. EVID. 401 (stating the standard for evidence to be considered "relevant").

186 *See* SCHEINDLIN & CAPRA, *supra* note 148, at 198-201.

187 FED. R. CIV. P. 34(b)(2)(D).

188 *Id*.

189 *See* FED. R. CIV. P. 34(b)(2)(B) ("For each item or category, the response must either state that inspection and related activities will be permitted as requested or state with specificity the grounds for objecting to the request, including the reasons.").

190 FED. R. CIV. P. 34(b)(2)(E).

191 FED. R. CIV. P. 34(b)(2)(E)(ii).

need to be presented in more than one form.[192] As such, counsel who requests access to Fitbit data must specify how they want the data to be presented, whether via e-mail, screenshots, printouts, or any other medium. Since Fitbit data is usually stored on the owner's computer, printouts from one's computer could be considered the form in which Fitbit data is ordinarily maintained.[193] When no form is specified, a specific—but not over-intrusive form—would have to be set as the form of delivery. In order to prevent the violation of a person's privacy in their Fitbit information, a screenshot of the requested data would be preferable.

Based on FRCP Rule 26, it also seems that the data stored on a Fitbit could fall under "initial required disclosure" because the party could use it to support his claim or defense.[194] However, it has only been seen in the Pennsylvania case as a form of discrediting a 911 caller's claim,[195] so potentially, the Fitbit data could not be entered under this section of the rule.

FRCP Rule 34 applies to electronically stored information and discusses what may generally be requested within the scope of Rule 26. Under Rule 34, electronically stored information includes "writings, drawings, graphs, charts, photographs, sound recording, images, and other data compilation-stored in *any medium* from which information can be obtained either directly or, if necessary, after translation by the responding party into a reasonably usable form."[196] The language of "any medium" seems overly broad, so to be clear the language should be amended to explicitly include Fitbits or similar wearable technology.[197] There should be a comment added to this rule explaining that in the circumstance of the medium being a wearable device like the Fitbit, it is obtainable. [198] However, there should be a strong emphasis on the "reasonably usable form" section to emphasize that the scope of the data should be strictly limited to that which is essential for the case at hand. [199] For instance, while Fitbit data can be converted into graphs and could potentially be considered data compilations, data compilations usually reflect statistics and not personal information, and it may be a stretch to include Fitbit data under that section.

---

192 FED. R. CIV. P. 34(b)(2)(E)(iii).
193 *Fitbug Ltd.*, 78 F.Supp.3d at1184.
194 FED R. CIV. P. 26(a)(1)(A)(ii).
195 *See* Hill, *Fitbit Data*, *supra* note 102.
196 FED. R. CIV. P. 34(a)(1)(A) (emphasis added).
197 FED R. CIV. P. 34.
198 *Id.*
199 FED R. CIV. P. 34(a)(1)(A).

V. POLICE WARRANTS, SEARCHES, AND SEIZURES THAT SHOULD APPLY TO FITBITS AND OTHER WEARABLE TECHNOLOGY

A. The Fourth Amendment to the U.S. Constitution

The Fourth Amendment of the Constitution protects the right of people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures.[200] The reasonableness of a search depends on whether the person who is subject to the search has a subjective expectation of privacy in the object being searched and that expectation is objectively reasonable.[201] Under the Fourth Amendment, warrants shall be issued only when there is "probable cause, supported by Oath or affirmation, and particularly describing the place to be searched and the person or things to be seized."[202]

B. Fourth Amendment Privacy Rights for Searches from the Police

By legal definition "[a] Fourth Amendment search occurs where the government, to obtain information, trespasses on a person's property to obtain information … [and] may also occur where the government violates a person's subjective expectation of privacy that society recognizes as reasonable to collect information."[203]

In this case, the police did not trespass on Ms. Risley's location because she called the police to assist her, but they did perform an illegal search when they searched her Fitbit.[204] In performing the search, the police arguably violated Ms. Risley's subjective expectation of privacy.[205] While not much case law exists about society having a subjective expectation of privacy to their Fitbits,[206] this is an area of the law that will expand in the future as data from Fitbits become more common in litigation. Fitbit users have clearly been appalled by their personal information being published without their consent in the past, and it is fair to say that Fitbit users have a reasonable expectation of privacy in the data monitored and stored by their Fitbits.

---

200 U.S. CONST. amend. IV, cl 1.

201 United States v. Wicks, 73 M.J. 93, 98 (C.A.A.F. 2014) (citing Katz v. United States, 389 U.S. 347, 361).

202 U.S. CONST. amend. IV.

203 United States v. Alabi, 943 F.Supp.2d 1201, 1264 (D.N.M. 2013).

204 *Id.* at 1233.

205 *Id.* at 1245.

206 Michelle M. Christovich, Note, *Why Should We Care What Fitbit Shares?: A Proposed Statutory Solution to Protect Personal Fitness Information*, 38 HASTINGS COMM. & ENT. L.J. 91, 97 (2016) ("Justice Sotomayor suggest, that users do not forfeit their reasonable expectation of privacy simply because they have shared fitness information with companies like Fitbit and Jawbone for limited health-related purposes.").

During a Fourth Amendment search, the issue will be whether the search is unreasonable.[207] In the case of a Fitbit, the search will essentially be about an item worn on someone's wrist and not just a laptop sitting on a table in someone's home. Consequently, the search parameters will have to be different. Furthermore, it has already been established that "files and folders contained as digital evidence on a hard drive are entitled to the same Fourth Amendment analysis as a filling cabinet containing documents and records."[208]

"A person has no legitimate expectation of privacy in information he voluntarily turns over to third parties."[209] Therefore, if a Fitbit user is ever faced with a Fourth Amendment violation, the party trying to obtain the data from the device might try to argue that because the wearer had set their privacy settings to public, they were voluntarily sharing their information with third parties and therefore had no reasonable expectation of privacy. The wearer should not lose their Fourth Amendment rights because most are unknowingly sharing their information with third parties. The voluntary sharing of information exception should not apply to uninformed Fitbit consumers sharing their information to third parties as has been seen in the past with consumer's personal sexual exploits being searchable through search engines.

C. Warrantless Searches

There are two types of warrants: arrest warrants and search warrants.[210] In order to receive a warrant the police officer must fulfill three essential requirements:

> [f]irst it must be issued by a *neutral and detached* magistrate. Second, there must be an adequate showing of *justification* to the magistrate, which is usually in the form of a sworn affidavit from a police officer…Finally, as required by the Fourth Amendment, the warrant must describe in a *particular* way 'the place to be searched and the persons or things to be seized.' [211]

To conduct a warrantless search, the police officer "must have a reasonable suspicion that a crime has been or is being committed."[212] There are four scenarios where the law will allow police to conduct warrantless searches: emergency, search incident exception, automobile exception, and plain view excep-

---

[207] *See* Crosswhite, *supra* note 60.
[208] United States v. Kim, 677 F.Supp.2d 930, 936 (S.D.Tex. 2009).
[209] *Smith*, 442 U.S. at 743-44.
[210] ROBERT M. BLOOM, SEARCHES, SEIZURES, AND WARRANTS, A REFERENCE GUIDE TO THE UNITED STATES CONSTITUTION 91 (2003).
[211] *Id.* at 92.
[212] ROBERT H. WOODY, SEARCH AND SEIZURE, THE FOURTEENTH AMENDMENT FOR LAW ENFORCEMENT OFFICERS 55 (2006).

tion.[213] The premise supporting these exceptions was the Supreme Court holding that "The Fourth Amendment does not require police officers to delay in the course of an investigation if to do so would gravely endanger their lives or the lives of others."[214] The following will discuss why none of these exceptions could be used to explain a legal warrantless search of a Fitbit.[215]

Certain exceptions, particularly the emergency assistance exception, allow for warrantless searches of homes and bodily fluids.[216] If an emergency situation was attempted as a defense in the *Risley* case, it would have to be applied to a search of Ms. Risley's boss' home, since there was no bodily fluids in the fact pattern. However, there was no emergency situation in *Risley*. The alleged intruder had already left, so there was no need for a warrantless search of the home. As such, no one was at risk of harm, including Ms. Risley and the police.[217]

The search incident to arrest exception is the oldest exception for a warrantless search and has "always [been] recognized under English and American law, to search the person of the accused when legally arrested to discover and seize the fruits or evidence of crime."[218] This exception was created to prevent the destruction of evidence as well as to protect police officers from potential danger.[219] However, the scope of the search the police could conduct has to be the "area within the arrestee's control … from within which he might gain possession of a weapon or destructive evidence."[220]

This exception could not be used in *Risley* because neither Ms. Risley, nor anyone else, was arrested at any point in the scenario.[221] Furthermore, the police cannot even argue that they examined the Fitbit as part of their "protective sweep" of the house.[222] Police officers are allowed to do full house searches as a protective sweep to check for accomplices that could pose a risk to their person.[223] However, these sweeps "should not last longer than is necessary to ad-

---

213 *See* BLOOM, *supra* note 210, at 101.

214 *See id.* at 103.

215 Brigham City v. Stuart, 547 U.S. 398, 403 (2006) ("Nevertheless, because the ultimate touchstone of the Fourth Amendment is 'reasonableness,' the warrant requirement is subject to certain exceptions.").

216 *See* BLOOM, *supra* note 210, at 102.

217 Sophie Aubrey, *Police Charge Woman for Making Up a Rape After She Was Exposed By Her Own Fitbit*, NEWS CORP. AUSTL. NETWORK (June 24, 2015, 6:38 PM), http://bit.ly/1U9Kw82.

218 Weeks v. United States, 232 U.S. 383, 392-93 (1914).

219 *See* WOODY, *supra* note 212, at 106.

220 Chimel v. California, 395 U.S. 752, 763 (1969).

221 *See* Aubrey, *supra* note 217.

222 *See* WOODY, *supra* note 212, at 108.

223 Maryland v. Buie, 494 U.S. 325, 335 n.3 (1990) ("A protective sweep is without question a 'search.'"); *see also* United States v. Burrows 48 F.3d 1011, 1015 (7th Cir. 1995) ("The same considerations that justify [pat searches] and [vehicle protective searches] ani-

dress the danger."[224] There is nothing in the facts to substantiate that the officers believed there were any accomplices in the home since Ms. Risley alleged that only one man had attacked her.[225] Moreover, there was no reason for the police officers to think they were in danger since there was nothing on the scene or the surrounding area of the guest home to give them any indication they were in harm's way.

The plain view exception doctrine grants the police the right to seize an item in their visual vicinity when engaged in a lawful arrest or search[226] This doctrine does not permit an extension of Fourth Amendment activity but only a "seizure of something discovered pursuant to a lawful intrusion … police may not search in an area not covered by a warrant or an exception to a warrant."[227] The police arrived at Ms. Risley's request, so that does not compromise a legal intrusion.[228] More importantly, this exception does not grant the police access to just search at their discretion.[229] As the Supreme Court established in *Coolidge*, "the plain view doctrine may not be used to extend a general exploratory search from one object to another until something incriminating at last emerges."[230] Just as it did not make sense for the police to search the defendant's stereo when searching for weapons in *Coolidge*, similarly, searching a Fitbit when a woman was allegedly raped, would not fall within the scope of the plain view exception.

D. Items Police Can Seize During a Search

Originally, the only possible evidence that police could seize had to be related to the crime, which excluded personal items.[231] However, the Supreme Court ruling in *Warden v. Hayden*, changed what could be seized to "all types of presumed evidence" because "the seizure of personal items was no more intrusive than seizing instruments, fruits, or contraband associated with the

---

mate the exception for the 'protective sweep.'").

224 *See* WOODY, *supra* note 212, at 108.

225 *See* Aubrey, *supra* note 217.

226 Coolidge v. New Hampshire, 403 U.S. 443, 465 (1971).

227 BLOOM, *supra* note 210, at 111-12.

228 State v. Bell, 737 P.2d 193, 201 (Wash. 1987). As held in this case if the privacy of the resident has been lawfully invaded it does not make legal sense to require a warrant for other officers to enter and complete the search.

229 *Coolidge*, 302 U.S. at 466 (explaining that officers cannot use a subjective standard when searching they must use an objective standard of conduct).

230 *Id*. (explaining that arriving at a person's request, such as a 911 call, grants the officers consent to enter the premises).

231 *See* WOODY, *supra* note 212, at 72-73.

crime, and that there should be no 'mere evidence' limitation."[232] However, in this scenario, when dealing with a woman's allegation that a man intruded into the house and raped her, the police wanting to seize her clothes, items from the scene, or possible evidence on Ms. Risley's person would have made sense, but obtaining her Fitbit did not. While Ms. Risley may have been lying in this case and the outcome was beneficial to serving justice, this by no means makes it legal for police to search and seize all Fitbits in the future.

VI. PROPOSED SOLUTION: RULES FOR ACCESSING WEARABLE TECHNOLOGY

A. Fourth Amendment Protection

The legal solution to the admissibility of Fitbit data should be analyzed through the same stringent test that other private items incur under the Fourth Amendment.[233] First, the police must be on the scene through a legal entry, which means they have been called onto the scene or the officers have probable cause to believe that a crime has or is occurring.[234] Second, once legally on the scene, police officer's searches must be carried out with a warrant or under one of the warrantless exceptions.[235] If a search is done without an arrest warrant, then the Fitbit must be on the person being arrested or within the area that person can immediately control. [236] But if in the future an officer were to specifically be at a location to search through the Fitbit's data then the search warrant must specify that in plain language. [237] If in the midst of that search, something is found, the police can only seize the item if it is specifically listed within the time and descriptions specifications of the warrant. [238]

Therefore, in the circumstances of Fitbits, the warrant must specify date, time, location, and specifically list out "Fitbit", "Apple Watch", or whatever other form of wearable technology the warrant was issued for. Most importantly, the scope of the warrant should specify the types and dates of data the police are able to access. [239] The data restrictions should be made specific to the time and day in which the unlawful act occurred. Going beyond that scope

---

232 *See id.* at 73.
233 *See Wicks*, 73 M.J. at 99.
234 *See* Wolf v. People of the State of Colorado, 338 U.S. 25, 27-28 (1949).
235 Payton v. New York, 445 U.S. 573, 581 (1980). The Supreme Court held that "the Fourth Amendment forbids policy entry into a private home to search for and seize an object without a warrant," except for when there are exigent circumstances present.
236 *Chimel*, 395 U.S.at 762-63.
237 Groh v. Ramirez, 540 U.S. 551, 557 (2004).
238 *Id.; see also* Maryland v. Garrison, 480 U.S. 79, 84 (1987).
239 *Garrison*, 480 U.S. at 84.

would be unjust and a huge invasion of privacy. [240]

B. Right to Privacy: Fitbit's Efforts to Protect Users

To solve the issue of a Fitbit owner's privacy expectancy, each client attempting to purchase a Fitbit should be more thoroughly aware about the possible risks of their personal data going public and given advice to "avoid connecting to third-party Wi-Fi and Bluetooth networks unless truly necessary."[241] As mentioned, people's personal sexual activity data has been exposed in the past and therefore there is a real possibility of very private Fitbit data being exposed to the public. That scandal occurred during the Fourth of July in 2011 when, "tech entrepreneur Andy Baio pointed out that Fitbit users' sexual activity was showing up in Google search results, the company has gone celibate.[242] Fitbit.com no longer offers any form of sex, which previously ranged from 'light effort' to 'vigorous' as a physical activity that users could track."[243] In that particular case, the issue was the default setting on the woman's Fitbit was set to share information with "anyone."[244] One possible solution could be for increased transparency regarding the default privacy settings of Fitbit.

The Fitbit default settings should be set to private and the owner may choose to change the settings to "anyone" rather than having the default settings placed the other way around. One should have the reasonable expectation that his or her personal wearable device should keep their personal information confidential, since most people buy wearable technology with the purpose of recording and monitoring their own physical excursion and not with the intention of sharing that sort of information with the public.

C. As Discoverable Evidence

To solve the issue of discovery in a criminal case, the Fitbit will have to be given a certain category in electronic discovery. The major legal challenge with this technology is that because of its newness judges are not clear as to

---

240 *See* Horton v. California, 498 U.S. 128, 138-39 (1990). An officer is not permitted to seize a second item not listed on the warrant based on their suspicion alone. Officers cannot expand the scope of the search and expect immunization for all items based on their subjective state of mind. Officers should instead use an objective standard of conduct.

241 Bromberg & Cranston, *supra* note 73, at 2.

242 Kashmir Hill, *No More Sex-ercise for Fitbit* Users, FORBES (July 12, 2011, 10:32 AM), http://onforb.es/1YSW68V.

243 *Id.*

244 *See* Hill, *Fitbit Moves Quickly*, *supra* note 58.

where it should fit.[245] Once there is a designated category for it, the legal community will be able to know what rules and laws should apply to it. Furthermore, specific rules of evidence should apply to wearable technology because that information can be very personal and should therefore be restricted to very specific parameters. The information requested must be reasonable and relevant within the scope of the legal issue at hand.

Wearable technology should not be assumed to be admissible evidence. A subpoena should be entered similarly for other technology that is to be entered into discovery. [246] In order to have grounds for the subpoena there must at least be probable cause that the wearable technology possesses information vital to the case at hand, which cannot be obtained from another source. [247] The data obtained from a Fitbit will have to be limited to the day and time of the alleged crime and all data relevant to times and days not in question should be off hands because of scope.[248]

VII. CONCLUSION

Every jurisdiction should update their rules governing the specifications for Fitbits and other wearable devices. Fitbits need to be placed in the same category as cell phone and computers, which require a warrant to be legally searched by police even incident to arrest. Wearable devices arguably hold an even higher level of privacy because it contains medical information about the wearer. Therefore, it should be considered analogous to a personal computer that has the capacity to contain highly sensitive and private information. Rules could potentially add wearable technology to one of the categories already stated in the Federal Rules of Evidence through the comments section. Hopefully, within the next decade, enough case law will exist to provide precedent on how data from this new technology should be used and permitted in litigation.

As for the Fitbit company, beyond changing their privacy policies, which they already did, they should change their default settings of information sharing to private and therefore allow people to change the setting to "anyone" if they so desire, instead of having to change it from public to private. If the Fitbit data passes all the strict regulations of admissibility, then an expert witness should be called to explain what each part of the data represents

---

[245] *See* John G. Browning, *Fitbit Data Brings Another Dimension to Evidence*, IADC COMM. NEWSL., July 2015, at 1, 4-6, http://bit.ly/1Tvfkht.

[246] In re Grand Jury Subpoena Duces Tecum, 846 F.Supp. 11, 12 (S.D.N.Y. 1994).

[247] See v. City of Seattle, 387 U.S. 541, 544-45 (1967).

[248] Warrants need to be specific about the "place to be searched and the things to be seized." *Horton*, 496 U.S. at 139-40.

in the context of its wearer and the litigation.