"OUTRUNNING" THE FOURTH AMENDMENT: A FUNCTIONAL APPROACH TO SEARCHES OF WEARABLE FITNESS TRACKING DEVICES

William Kendall*

I. INTRODUCTION

Suppose a resident reports a burglary late at night to the police. The resident tells the responding officer he chased off the burglar, and in doing so observed what he believed was a middle-aged man, wearing sweatpants and a long-sleeved shirt. The resident indicates the man ran down the street heading north. The officer immediately radios the description to patrol units who began to search the area. Initially, the police were unable to locate the suspect. However, through investigation and canvassing, they gather just enough probable cause to arrest a man who is believed to be the suspect.

Upon arrest, police note he is wearing a digital fitness tracker[1] and conduct a search incident to arrest. The search yields evidence of the suspect's heart rate, sleep activity, distance traveled, and calories burned over the last five days. In a statement and at trial the suspect acknowledged wearing the tracker at all times except to charge it every three to five days. Further, he contends he was at home asleep at the time of the incident in question. Using the fitness tracker data, prosecution is able to show the suspect had an elevated heart rate consistent with vigorous physical activity and that the suspect was awake two hours before the burglary and two hours after.

The suspect asserts police should be required to obtain a warrant before searching *any* digital device, and therefore the search was unlawful. The government contends their prized evidence was obtained lawfully and such a search is constitutional under a *Riley v. California* application.[2]

---

* William Kendall is a third-year law student at Southern Illinois University School of Law. Prior to becoming a law student, he was a criminal investigator with the Marine Corps Criminal Investigation Division (CID). He would like to thank his faculty advisor, Professor Edward Dawson, for his guidance and feedback. He would also like to thank the men and women of law enforcement and those who provided support and encouragement throughout the writing process.

1 Hereinafter referred to as "fitness tracker" or "tracker" for continuity and reader's ease. These devices are often referred to by many names such as "wearable" and "smartwatch" or often by their respective brand name such as, "FitBit" or "Garmin."

2 *See* Riley v. California, 134 S. Ct. 2473 (2014) (the Court held cell phones enjoyed protections under the Fourth Amendment, and despite the general exception to the warrant requirement for

The U.S. Supreme Court has said generally law enforcement may search items found on an arrestee upon a lawful arrest,[3] but in *Riley*, the Court made an exception to the rule and held police may not search a cell phone without first obtaining a warrant.[4] The Court largely based the *Riley* exception on the large amount of personal, private data contained in a person's cell phone.[5] Although the *Riley* decision has commanded an exception to the search incident to arrest rule, in that police must generally obtain a warrant to search a cell phone, it fails to specify whether a warrant should be required for other digital devices such as fitness trackers, and other wearable data-containing devices.[6]

This Note applies *Riley* and other cases to fitness trackers and argues that a blanket rule, which would require police to obtain a warrant prior to searching *any* digital device found on an arrestee at the time of arrest, is not in line with the Court's search and seizure precedent. Instead, as in *Riley*,[7] the appropriate rule is a narrowly tailored rule, easy to apply in the field, which allows a workable balance between government interest and interest of the people.

Upon locating a wearable data device on an arrestee, the police officer would make a field determination as to whether the device shared "advanced" or often thought of as "smart" features similar to the characteristics to that of a modern cell phone: that is, if it had similar characteristics as those contemplated in *Riley*.[8] If the device shares those same characteristics, the officer would be required to obtain a warrant before searching the device. Categories would be based on the device's capability, the information it contains, and its connectivity to other information, among other elements outlined in *Riley*.[9] In arguing for this approach, this Note challenges other scholars' proposals for a bright-line rule that would create a sweeping ban forcing law enforcement to secure a warrant to search *all* digital devices found on an arrestee.[10] This Note proposes that a functional rule would favor

---

searches incident to an arrest, searches of cell phones would require a warrant absent exigent circumstances).

3 Chimel v. California, 395 U.S. 752, 762–63 (1969) ("When an arrest is made, it is reasonable for the arresting officer to search the person arrested in order to remove any weapons that the latter might seek to use in order to resist arrest or effect his escape . . . [i]n addition, it is entirely reasonable for the arresting officer to search for and seize any evidence on the arrestee's person in order to prevent its concealment or destruction.").

4 *See Riley*, 134 S. Ct. 2473.

5 *Id*.

6 *Id*.

7 *Id*.

8 *Id*. at 2489–91.

9 *Id*.

10 *See, e.g.*, Katharine Saphner, *You Should Be Free to Talk the Talk and Walk the Walk: Applying* Riley v. California *to Smart Activity Trackers*, 100 MINN. L. REV. 1689, 1723 (2016); *see also* Pat Augustine, *Wearable Evidence: Why the Pennsylvania Judiciary Should Require a Warrant to Search Wearable Technology*, 17 U. PITT. J. TECH. L. & POL'Y 1, 16 (2017) ("As a result, the

legitimate government interests and simultaneously preserve the privacy interest of the people.

Part II of this note explores the variety and functionality of fitness trackers and provides data related to the number of users and devices shipped from manufacturers. It also surveys instances where fitness trackers have gained popularity through employers and where fitness trackers have surfaced in the law. Part III reviews the Fourth Amendment, the exception to the general warrant requirement when police search an arrestee, and the holding in *Riley* as it pertains to the search of digital devices found on an arrestee upon a lawful arrest.[11] Part III also surveys cases in which lower courts have applied *Riley* to other digital devices, such as cameras, gift cards, and iPods. Finally, Part IV provides the proposed rule based on the categories of devices, one rooted in both legitimate government interests and protections of citizens' privacy, and gives examples of how that rule would work in practice to further the policies that are the basis for the *Riley* rule.

II. BACKGROUND

This part will first explore the basics of fitness trackers, displaying the variety and functionality of the devices. Second, this part will connect the functionality of fitness trackers with how they have been and could be used in legal matters.

A. Fitness Trackers: What They Do and How They Vary

Not all fitness trackers are the same. There are a wide variety of fitness trackers that claim a range of capabilities, some nearing simple pedometers, while others have cutting edge smart watch features.[12] This Note does not attempt to describe all fitness trackers but rather the specific features associated with common fitness trackers and how they may serve as a marker in applying a search incident to arrest rule based on capabilities of the tracker itself.

Smartwatches and fitness trackers sold at a record high of 102.4 million devices in 2016.[13] Fitbit, Inc. devices accounted for nearly twenty-two percent of the devices shipped. Apple made up approximately 10.5%,

---

Pennsylvania judiciary must require law enforcement to obtain a warrant before searching wearable technology.").

11 *See Riley*, 134 S. Ct. 2473.

12 *See generally* Robin Hilmantel, *I Tested 7 Different Fitness Trackers-at the Same Time*, WOMEN'S HEALTH (Jan. 1, 2016), https://www.womenshealthmag.com/fitness/fitness-tracker-reviews (compares several different fitness tracking devices).

13 Dan Graziano, *Fitbit Sold More Wearables in 2016 than Apple and Samsung Combined*, CNET (Mar. 2, 2017, 7:15 AM), https://www.cnet.com/news/fitbit-sold-more-wearables-in-2016-than-apple-and-samsung-combined/ (citing information provided by International Data Corporation).

Garmin approximately 5.9%, and Samsung comprised around 4.3% of the total units shipped in 2016.[14]

Fitbit, Inc. reported in 2016 it sold 22.3 million devices with 23.2 million active Fitbit users.[15] These numbers come despite the twelve percent increase in average selling price of their devices from the third quarter in 2016 to the third quarter in 2017.[16] Currently, Fitbit, Inc. sells six different trackers that range from a clip-on tracking device called the "Zip," to the recently released "Ionic."[17]

The "Zip" is advertised to track steps, calories, and distance with a feature to provide the date and time.[18] The "Alta HR," with a midrange price point in comparison to the other five trackers, is advertised to provide the end-user with the same information as the "Zip" along with sleep tracking, heart rate tracking, call and text notifications, and calendar alerts, among other features.[19] The Fitbit, Inc., "Ionic" fitness tracker is, at the time of this Note, the highest priced model advertising the most features.[20] The "Ionic" is advertised to be capable of providing the end-user with all the features included on the "Zip" and "Alta HR" but also includes tracking for the number of floors climbed, has built-in GPS, allows users to download and use applications, stores and plays music, and even provides the user the ability to make payments.[21] The "Ionic" contains an altimeter, 3-axis accelerometers, digital compass, GPS, optical heart rate monitor, ambient light sensors, and is advertised to record heart rate data at one-second intervals during exercise and at five seconds in normal use.[22]

Fitness trackers often vary in their ability to internally store data without rewriting or needing to offload the data to an application. For instance, the Fitbit, Inc. "Zip" is marketed to track seven days of "detailed motion data – minute by minute."[23] The "Ionic" boasts a seven-day memory of "detailed

---

14 *Id*.

15 *Fitbit Reports $574M Q416 and $2.17B FY16 Revenue, Sells 6.5M Devices in Q416 and 22.3M Devices in FY16*, FITBIT (Feb. 22, 2017), https://investor.fitbit.com/press/press-releases/press-release-details/2017/Fitbit-Reports-574M-Q416-and-217B-FY16-Revenue-Sells-65M-devices-in-Q416-and-223M-devices-in-FY16/default.aspx.

16 *Fitbit Reports Third Quarter Results*, FITBIT (Nov. 1, 2017), https://investor.fitbit.com/press/press-releases/press-release-details/2017/Fitbit-Reports-Third-Quarter-Results/default.aspx.

17 *Fitbit Store: Buy Ionic, Blaze, Charge 2, Flex 2, Zip, Aria 2 & Flyer*, FITBIT, https://www.fitbit.com/store (last visited Nov. 4, 2017).

18 *Id*.

19 *Id*.

20 *Id*.

21 *Id*.

22 *FitBit Ionic Watch*, FITBIT, https://www.fitbit.com/ionic (last visited Nov. 6, 2017).

23 *FitBit One: Wireless Activity + Sleep Tracker*, FITBIT, https://www.fitbit.com/one#specs (last visited Nov. 5, 2017).

motion data . . .” which includes “daily totals for past 30 days.”[24] Overall, the “Ionic” is marketed to have an internal memory of 2.5 gigabytes.[25]

B. Fitness Trackers: Running Into Law

The features often associated with fitness trackers, such as heart rate monitoring, sleep tracking, and movement data, have caused concerns due to the medical-like data that is tracked and stored.[26] Fitness trackers have found growing use in corporate wellness programs, which incentivize employee wellness.[27] Companies have found by using fitness trackers, participation has increased significantly.[28] Among those utilizing fitness trackers for discounts on health insurance are employers such as BP and eBay.[29] Such programs are another example of the popularity of these devices not only for private use, but for use by employers as well.

In response to employers’ push to get employees to utilize the fitness tracking programs, employees have raised concern about the data collected and how it may be used against them.[30] Specifically, employers who provide employees with fitness trackers may track data 24/7, not just at work.[31] Such concerns by employees exemplifies the want for protections in personal data, specifically here, fitness tracking data. The Court in *Riley* recognized a need for protection of arguably similar private data found within a cell phone.[32]

Beyond private use and the use of tracker data for insurance savings by employers,[33] police and attorneys have used fitness tracker data in criminal cases,[34] further bringing fitness tracker data into the legal spectrum. In one

---

24 FitBit Ionic Watch, *supra* note 22.

25 Fitbit Ionic - Smartwatch Specifications, SMARTWATCH SPECIFICATIONS, http://www.smartwatchspecifications.com/Device/fitbit-ionic/ (last visited Nov. 5, 2017).

26 Rodika Tollefson, *Fitness Trackers can be Dangerous to the Health of your Data*, THIRD CERTAINTY (Jan. 30, 2017), http://thirdcertainty.com/featured-story/fitness-trackers-can-dangerous-health-data/; *see also* Alexandra Troiano, *Wearables and Personal Health Data Putting A Premium on Your Privacy*, 82 BROOK. L. REV. 1715, 1718 (2017).

27 *mHealth Wearables Help Employers Achieve Higher Corporate Wellness Participation Rates*, ABIRESEARCH (Sep. 26, 2016), https://www.abiresearch.com/press/mhealth-wearables-help-employers-achieve-higher-co/; *see also* Troiano, *supra note* 26, at 1715.

28 *mHealth Wearables Help Employers Achieve Higher Corporate Wellness Participation Rates*, *id.* note 27 (“Early data suggests that corporate wellness programs with wearable devices increase average employee participation from 20 percent to between 60 and 70 percent, with some employers reporting participation rates above 90 percent.”).

29 Naomi Sansom, *Wearable Technology in the Workplace*, 20 No. 2 GLCYLAW 6, 1 (2015).

30 Ifeoma Ajunwa et al., *Limitless Worker Surveillance*, 105 CALIF. L. REV. 735, 766–67 (2017).

31 *Id.* at 772.

32 Riley v. California, 134 S. Ct. 2473, 2489 (2014) (discussing privacy concern in the plethora of data contained on a cell phone.).

33 Sansom, supra note 29.

34 Alejandro Alba, Police, *Attorneys are Using Fitness Trackers as Court Evidence*, N.Y. DAILY NEWS (Apr. 19, 2016), http://www.nydailynews.com/news/national/police-attorneys-fitness-trackers-court-evidence-article-1.2607432.

case, law enforcement used an alleged victim's fitness tracking data from a Fitbit "Surge" to determine she was not forced out of her bed and raped, but instead was walking around all night staging a crime scene.[35]

In a Connecticut murder case in December 2015, detectives used fitness tracker data to help establish the timeline and movement of a woman believed to be murdered by her husband.[36] In this case, police sought and obtained a warrant for the fitness tracker which contained specific information such as when the victim had moved, the distance recorded in a certain time frame, and when the movement subsided.[37]

Fitness trackers with GPS tracking capabilities can also provide the user's run route, which can be overlaid on an aerial photograph.[38] For instance, a jogger, four miles into her ten-mile route, reported she was attacked in Seattle, Washington.[39] The jogger posted pictures of her face showing blood and lacerations as well as an aerial photograph that depicts a red line where her GPS enabled fitness tracker logged her attempt to evade her attacker.[40] Subsequently, the suspect, reportedly a registered sex offender who had a history of violence toward women, was arrested for attempted rape in the second degree and second-degree assault.[41] While both of the aforementioned cases involved a victim, it is easy to imagine how tracker data could be relevant in identifying or incriminating suspects.[42]

Fitness trackers have also been introduced as evidence in personal injury cases, further exemplifying popularity of this type of data to be used as evidence in the court. Attorneys used data obtained from the fitness tracker as evidence to show how her normal activity had changed after being injured.[43] In such a case, the comparative activity logged before and after an injury served as evidence to show whether the victim had an increase or decrease in physical activity.[44]

---

35 *Id*.

36 Amanda Watts, *Cops Use Murdered Woman's Fitbit to Charge Her Husband*, CNN (Apr. 26, 2017), http://www.cnn.com/2017/04/25/us/fitbit-womans-death-investigation-trnd/index.html.

37 *Id*.

38 Melinda Carstensen, *A Jogger's Fitness Tracker Documented Her Brutal Attack on a Run*, FOX NEWS LIFESTYLE (Mar. 14, 2017), http://www.foxnews.com/lifestyle/2017/03/14/joggers-fitness-tracker-documented-her-brutal-attack-on-run.html.

39 *Id*.

40 *Id*.

41 *Id*.

42 *See generally* United States v. Carpenter, 819 F.3d 880 (6th Cir. 2016), *cert. granted*, 137 S. Ct. 2211 (2017); United States v. Jones, 565 U.S. 400 (2012).

43 Alba, *supra* note 34.

44 *Id*.

III. 4TH AMENDMENT LAW GOVERNING SEARCHES OF TRACKERS

It is clear the Framers of the U.S. Constitution did not contemplate a situation wherein a police officer would need to decide whether a search of a fitness tracker is constitutional. That is unless one considers the Court's stealthy and patient stowaway-constable as discussed in *United States v. Jones*[45] as similar to the capability of today's modern fitness tracking device. Thankfully, however, modern day Fourth Amendment jurisprudence provides some guidance on how to approach the very difficult question.[46]

A. Fourth Amendment Basics—Reasonableness and Warrant Requirements

The Fourth Amendment of the U.S. Constitution provides for a right that people be "secure in their persons, houses, papers, and effects, against unreasonable searches and seizures . . . and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized."[47] Since the birth of the Fourth Amendment, courts have interpreted and molded the present day application of what constitutes a lawful search.[48]

In large part, the courts have determined "the text of the Fourth Amendment indicates, the ultimate measure of the constitutionality of a governmental search is 'reasonableness.'"[49] In its application of reasonableness, the U.S. Supreme Court has held generally a warrant is required for searches by law enforcement unless the search falls under an exception.[50] One of the Court's recognized exceptions to the general warrant requirement is the search incident to a lawful arrest.[51]

B. General Rule Allowing Warrantless Searches of Worn Containers Found on Arrestees' Persons

As recognized by the U.S. Supreme Court, "because the ultimate touchstone of the Fourth Amendment is 'reasonableness,' the warrant requirement is subject to certain exceptions."[52] One such exception is the search incident to arrest, which is reviewed by the Court in *Riley* and dubbed

---

45 *See Jones*, 565 U.S. at 406 n.3.

46 *See* Riley v. California, 134 S. Ct. 2473 (2014).

47 U.S. CONST. amend. IV.

48 *See, e.g.*, Orin S. Kerr, *The Curious History of Fourth Amendment Searches*, 2012 SUP. CT. REV. 67.

49 Vernonia Sch. Dist. 47J v. Acton, 515 U.S. 646, 652 (1995).

50 *Riley*, 134 S. Ct. at 2482.

51 Chimel v. California, 395 U.S. 752, 762–63 (1969).

52 Brigham City v. Stuart, 547 U.S. 398, 403 (2006).

the "search incident to arrest trilogy."[53] A brief synopsis of the "trilogy"[54] is explored in this section.

1. Chimel v. California

The U.S. Supreme Court emphasized a prudential exclusion to the general warrant requirement under the Fourth Amendment in *Chimel v. California*, wherein the Court specifying officer safety and preservation of evidence reasons held a police officer may search the persons of the arrestee in order to remove weapons and seize evidence.[55] Mr. Ted Chimel was the subject of an arrest warrant for two charges of burglary.[56] Upon finding Mr. Chimel's home, the police entered and waited for Mr. Chimel to arrive.[57] Upon his arrival, police advised Mr. Chimel of the arrest warrant and asked for consent to "look around," which Mr. Chimel protested.[58] Police advised Mr. Chimel they could conduct a search anyway because of the search incident to arrest exception.[59] Police began searching the entire home, including the attic, garage, and workshop wherein numerous items were seized and used against Mr. Chimel at trial.[60]

The Court held law enforcement exceeded the scope of the search allowable under the exception that a warrant is not required to search an arrestee's person, and his immediate area, when they searched throughout the home.[61] In this case, the police officers exceeded their allowable scope and therefore the Court found the search to be "unreasonable" and invalid.[62] The Court reasoned searching beyond the area where Mr. Chimel was arrested exceeded the scope of the allowable search because he could not have reached the areas (the attic, garage and workshop) to destroy evidence nor could the police officers have sufficiently alleged he had access to a weapon in these places at the time of arrest.[63]

---

53 *Riley*, 134 S. Ct. at 2484.

54 *See Chimel*, 395 U.S. at 752; United States v. Robinson, 414 U.S. 218 (1973); Arizona v. Gant, 556 U.S. 332 (2009). (Referred to in *Riley v. California* as "the trilogy[,]" a line of cases regarding search incident to arrest prior to *Riley*.) *Riley*, 134 S. Ct. at 2484.

55 *Chimel*, 395 U.S. at 762–63 (the Court also concludes that a search of the area within an arrestee's reach).

56 *Id*. at 753.

57 *Id*.

58 *Id*.

59 *Id*. at 753–54.

60 *Id*. at 753–55.

61 *Id*. at 768 ("The search here went far beyond the petitioner's person and the area from within which he might have obtained either a weapon or something that could have been used as evidence against him.").

62 *Id*. ("The scope of the search was, therefore, 'unreasonable' under the Fourth and Fourteenth Amendments and the petitioner's conviction cannot stand.").

63 *Id*. at 763–64.

2. United States v. Robinson

In 1973, the U.S. Supreme Court applied the *Chimel* analysis in *United States v. Robinson*, a case involving an arrest for driving with a revoked driver's license.[64] When the officer conducted a pat down of Mr. Willie Robinson Jr., he felt an object in Mr. Robinson's coat pocket.[65] The officer removed the object finding it to be a crushed cigarette package.[66] The officer opened the crushed cigarette pack and found heroin inside the pack.[67]

The Court acknowledged the reasoning in *Chimel*, holding it is reasonable for a police officer to search an arrestee to remove weapons and to preserve evidence.[68] The Court held the search of Mr. Robinson's person was lawful and the subsequent inspection of the cigarette package was valid, to include subsequent seizure of it upon finding heroin capsules inside.[69] In reaching this conclusion, the Court found the valid custodial arrest gave authority for police to conduct a full search of Mr. Robinson, and upon such a search police were allowed to inspect objects found on Mr. Robinson's person in order to "disarm" and "preserve evidence."[70]

3. Arizona v. Gant

In 2009, the U.S. Supreme Court expanded and further validated the search incident to arrest exception from *Chimel* when it decided *Arizona v. Gant*.[71] Like Mr. Robinson, Mr. Rodney Gant was arrested for driving with a suspended license and subject to a search; however, in *Gant*, the search was extended to Mr. Gant's car.[72] There, police located a jacket in the backseat, and upon search of the jacket, the police found cocaine inside the jacket pocket.[73]

The Court concluded, "[p]olice may search a vehicle incident to a recent occupant's arrest only if the arrestee is within reaching distance of the passenger compartment at the time of the search or it is reasonable to believe the vehicle contains evidence of the offense of arrest."[74] The Court posited this outcome by providing that a limitation exists to the search incident to arrest exception where an arrestee can no longer reach the area because he is

---

64 United States v. Robinson, 414 U.S. 218, 219–23 (1973).
65 *Id*. at 223.
66 *Id*.
67 *Id*.
68 *Id*. at 225–26.
69 *Id*. at 236–37.
70 *Id*. at 234.
71 Arizona v. Gant, 556 U.S. 332, 339 (2009).
72 *Id*. at 335.
73 *Id*.
74 *Id*. at 351.

in custody.[75] Once the arrestee is secured from the vehicle, he or she is unable to reach into the vehicle to destroy evidence or brandish a weapon; therefore, the justifications of preserving evidence and officer safety no longer give rise to the search incident to arrest exception.[76]

C. The *Riley* Exception—Warrant Required to Search Cell Phones Found on Arrestees' Persons

In 2014, the U.S. Supreme Court decided *Riley v. California*, in which the Court determined police officers must generally obtain a warrant to search a cell phone found on an arrestee, absent exigent circumstances.[77] *Riley* remains the Court's current keystone regarding the search of digital devices, specifically cell phones, incident to a lawful arrest.[78]

In *Riley*, the Court granted certiorari, consolidating two cases to decide whether law enforcement may search a cell phone that was seized from a person who was lawfully arrested.[79] The police searched a "smart phone" in one case and a "flip phone" (or dumb-phone) in the other.[80] The Court described a "smart phone" as "a cell phone with a broad range of other functions based on advanced computing capability, large storage capacity, and Internet connectivity" and a "flip phone" as "a kind of phone that is flipped open for use and that generally has a smaller range of features than a smart phone."[81] In both cases, police searched and seized evidence from the arrestee's cell phone (seized from their person) and the resulting evidence was used in their conviction.[82]

The Court recognized the holdings in *Chimel*, *Gant*, *and Robinson*[83] that a search incident to arrest was rooted in officer safety and preservation of evidence,[84] and yet decided, despite those concerns, a warrant should be required for the search of cell phones.[85] The Court found the privacy interest

---

75 *Id*. at 339.

76 *Id*.

77 *See generally* Riley v. California, 134 S. Ct. 2473 (2014) (the Court held cell phones enjoyed protections under the Fourth Amendment, and despite the general exception to the warrant requirement for searches incident to an arrest, searches of cell phones would require a warrant absent exigent circumstances).

78 *Id*.

79 *Id*. at 2482.

80 *Id*. at 2480–81.

81 *Id*.

82 *Id*. at 2480–82.

83 *Id*. at 2484 ("*Gant* . . . recognized that the *Chimel* concerns for officer safety and evidence preservation underlie the search incident to arrest exception." (citing Arizona v. Gant, 556 U.S. 332, 338 (2009))).

84 *Id*.

85 *Id*. at 2485.

associated with the amount of digital data and access to data in a cell phone outweighed the government interest in both cases.[86]

The Court, in contemplating the officer safety and preservation of evidence concerns discussed in *Chimel*, *Gant*, and *Robinson*, stated officers remain free to examine the outside of the cell phone to evaluate if it may contain a weapon, such as a blade; however, the data on the cell phone is not in itself a danger to anyone.[87] The Court found a government interest in the data on a cell phone in that it may alert police "that confederates of the arrestee are headed to the scene[,]" but the Court seemed unimpressed by the evidence presented that such a concern was "based on actual experience."[88] The Court further held there may be an exception to the warrant requirement wherein officer safety provides justification but contemplating exigent circumstances should be done case by case.[89]

In focusing on preservation of evidence concerns normally associated with search incident to arrest, the Court found that in both factual situations police could have secured the cell phones and sought a warrant, which would have removed the arrestees' ability to destroy data contained on the cell phone.[90] Further, the Court acknowledged the possibility for cell phones to be remotely wiped and provided that officers had concerns of such a possibility, they could circumvent the deletion of data by powering off the phone, removing the battery, or placing it in a Faraday bag to remove the cell phone from radio waves thereby blocking its signal.[91]

After contemplating the interest of the government in searching a phone and its relation to officer safety and preservation of evidence, the Court turned to the privacy interest in a person's cell phone and stated, "[c]ell phones differ in both a quantitative and a qualitative sense from other objects that might be kept on an arrestee's person."[92] The Court highlighted some of the elements that make a cell phone unlike that of the cigarette pack contemplated in *Robinson*.[93] The Court first noted, "many [cell phones] are in fact minicomputers that also happen to have the capacity to be used as a telephone[,] [t]hey could just as easily be called cameras, video players, rolodexes, calendars, tape recorders, libraries, diaries, albums, televisions, maps, or newspapers."[94] The Court recognized the storage on a cell phone poses privacy concerns in that "a cell phone collects in one place many distinct types of information—an address, a note, a prescription, a bank

---

86 *Id*. at 2493.
87 *Id*. at 2485.
88 *Id*.
89 *Id*. at 2486.
90 *Id*.
91 *Id*. at 2487.
92 *Id*. at 2489.
93 *Id*. at 2488–91.
94 *Id*. at 2489.

statement, a video—that reveal much more in combination than any isolated record."[95]

The Court stated, "[t]he sum of an individual's private life can be reconstructed through a thousand photographs labeled with dates, locations, and descriptions; the same cannot be said of a photograph or two of loved ones tucked into a wallet" which is in part due to the storage capacity of a cell phone.[96] In modern times, cell phones allow people to "carry a cache of sensitive personal information with them as they [go] about their day."[97]

The Court even went as far as making a comparison to the ever-sacred search of a home.[98] In doing so, the Court held, "[a] phone not only contains in digital form many sensitive records previously found in the home; it also contains a broad array of private information never found in a home in any form—unless the phone is."[99] The Court noted, "it is no exaggeration to say that many of the more than 90% of American adults who own a cell phone keep on their person a digital record of nearly every aspect of their lives…"[100]

The Court also found cell phones present another factor of privacy concern through the use of application software found on an increasing number of smartphones, which allow users access to information not stored on the device itself.[101] The Court ultimately found the search incident to arrest exception did not apply to cell phones, although other warrantless searches may be allowed under "other case-specific exceptions," such as when police are compelled by exigent circumstances.[102]

The Court concluded with a sentence that has already become regularly cited: "[o]ur answer to the question of what police must do before searching a cell phone seized incident to an arrest is accordingly simple—get a warrant."[103]

D. Lower Courts Wrestle with Applying Riley to Other Digital Devices

Following the *Riley* decision, courts have wrestled with applying the *Riley* warrant requirement and the Court's reasoning to other digital devices. Although fitness trackers are not the subject of the cases, this section surveys

---

95 *Id*.

96 *Id*.

97 *Id*. at 2490.

98 *Id*. at 2491.

99 *Id*.

100 *Id*. at 2490.

101 *Id*. at 2490–91 ("Mobile application software on a cell phone, or 'apps,' offer a range of tools for managing detailed information about all aspects of a person's life.") ("Such a search would be like finding a key in a suspect's pocket and arguing that it allowed law enforcement to unlock and search a house.").

102 *Id*. at 2494.

103 *Id*. at 2495 (A Westlaw search indicated this quote had been cited in more than 38 cases at the time of the inquiry).

lower court cases and provides insight into how the *Riley* holding is being applied on varying digital devices.

1. United States v. Turner

In *United States v. Turner*, the Fifth Circuit Court of Appeals applied the holding in *Riley* and found the scanning of stolen gift cards seized from a vehicle, without a warrant, did not amount to an unlawful search.[104] There, the Fifth Circuit held there was no reasonable expectation to privacy in gift cards since they do not have the quantifiable features that a modern cell phone has.[105] The court found gift cards lacked the storage capacity of a modern cell phone and that gift cards did not store the same types of information deemed to be held sacred in *Riley*, such as the amount of data and type of personal data found on a typical cell phone.[106] Instead, all the gift cards store are a "few lines of characters" and are "infinitesimally smaller" in memory storage than a typical cell phone.[107]

2. United States v. Miller

In *United States v. Miller*, the U.S. District Court for the Eastern District of Michigan, Southern Division, held a search of a digital camera does not equate to the search of a smart phone and did not require a warrant.[108] There, the defendant attempted to use *Riley* to exclude the search of a digital camera containing child pornography that was seized and searched pursuant to a search warrant of the home.[109] The court, although distinguishing the search type from *Riley*, held, "cameras contain a limited type of data, restricted to image and video files, that do not touch the breadth or depth of information that a cell phone's data offers."[110] Further, "[d]igital cameras also hold significantly less data than many cell phones—Defendant's camera had a total capacity of 2 gigabytes, while many common cell phones are able to hold 8 or 16, or even 64 gigabytes of information."[111] It should be noted it

---

104 United States v. Turner, 839 F.3d 429, 435–36 (5th Cir. 2016).

105 *Id*.

106 *Id*. (the court also discusses the difference between the purpose of the modern cell phone and a gift card, finding the cell phone to have a more complex purpose than a gift card that transferred information from the card to the seller).

107 *Id*. at 435.

108 United States v. Miller, 34 F. Supp. 3d 695, 700 (E.D. Mich. 2014) ("*Riley* is both factually and legally distinguishable. First, *Riley* involved a warrantless search incident to arrest, while this case involves a warranted search of a home. A different mode of analysis pertains to each. Second, the search of Defendant's camera does not raise the same privacy concerns as a cell phone.").

109 *Id*. at 696–97 (here, the court even ordered supplemental briefings following the *Riley* decision by the U.S. Supreme Court in order to consider the impact on the case).

110 *Id*. at 700.

111 *Id*.

was not contemplated whether a digital camera with internet connectivity (to social media, or wireless storage), and GPS capabilities would be treated the same as the camera in *Miller*.[112]

3. United States v. Jackson

In *United States v. Jackson*, the Eighth Circuit Court of Appeals declined to apply the *Riley* warrant requirement for the search of cell phones to Mr. Richard Jackson who was on supervised release.[113] The court determined Mr. Jackson's diminished right to privacy as a result of his supervised release allowed police to conduct a search of Mr. Jackson's cell phone because of the superseding governmental interest.[114] The court here distinguished this search from the search conducted in *Riley*, finding the parolee in this case had "clear notice" he was subject to such a search, and the supervised release conditions (which allowed the search of his cell phone) were a sanction brought by the court upon finding him guilty of criminal conduct.[115] This positioned the government's interest above the privacy interest of Mr. Jackson and as the court stated here, *Riley* was based on the search of an arrestee, not an offender under supervised release.[116]

4. United States v. Saboonchi

Just days after the U.S. Supreme Court decided *Riley*, the United States District Court for the District of Maryland applied *Riley* to a U.S. border search of a person's iPhone.[117]

In doing so, the court stated, "*Riley* held unequivocally that digital data is not subject to the warrant exception for searches incident to arrest and that, as a general matter, law enforcement officers must obtain a warrant before searching the contents of an arrestee's electronic devices."[118] In an example of the lack of clarity on how to apply *Riley*, it is noted in *Saboonchi* the court cited to *Riley* but stated, "law enforcement officers must obtain a warrant before searching the contents of an arrestee's *electronic devices*."[119] However, in *Riley*, the U.S. Supreme Court determined police must obtain a warrant in order to search a *cell phone* seized incident to arrest (not for *all*

---

112 *Id*.
113 United States v. Jackson, 866 F.3d 982, 985–86 (8th Cir. 2017).
114 *Id*.
115 *Id*.
116 *Id*.
117 United States v. Saboonchi, 48 F. Supp. 3d 815, 816–17 (D. Md. 2014).
118 *Id*. at 817.
119 *Id*.

digital data).[120] Nevertheless, the court applied an exception related to searches conducted at borders entering the United States and denied Mr. Saboonchi's motion to reconsider.[121]

5. People v. Folsom

In 2017, the Colorado Court of Appeals heard an appeal regarding the search and seizure of two iPods found on Mr. Nimroid Folsom's person during his arrest for stalking and attempted invasion of privacy for sexual gratification.[122] Without a warrant, police searched both iPods upon Mr. Folsom's arrest and discovered seventeen videos depicting "fully clothed women walking in public places—the videos focused on the lower half of the women's bodies . . . [and] a partially clothed woman changing clothing and masturbating in a bedroom."[123]

The court stated, "[n]ot surprisingly, the application of the Fourth Amendment to advanced technological devices—some of which are, in reality, portable computers with amazing storage and other capabilities—has been difficult."[124] Further, the court, in its own interpretation of *Riley*, stated, "[w]hile ordinarily the police may search a person incident to arrest and seize contraband or other evidence of a crime without further justification, courts have recognized that the warrantless seizure of a *person's computer or similar device* raises acute Fourth Amendment issues."[125]

The court, in applying *Riley*, determined the admission of videos at trial that were found on the iPods violated the Fourth Amendment because an iPod was the "equivalent" to a cell phone as discussed in *Riley*.[126] The court stated, "While an iPod does not have telephonic capabilities, the arresting officer testified that the iPods in this case could store videos, photographs, and music, and access the internet" and as a result enjoyed the same protections as a cell phone.[127]

---

120 Riley v. California, 134 S. Ct. 2473, 2495 (2014) ("Our answer to the question of what police must do before searching a cell phone seized incident to an arrest is accordingly simple—get a warrant.").

121 United States v. Saboonchi, 48 F. Supp. 3d 815, 817–20 (D. Md. 2014).

122 People v. Folsom, 2017 COA 146M, ¶¶ 1-11, *as modified on denial of reh'g* (Colo. App. Dec. 28, 2017).

123 *Id.* ¶ 10.

124 *Id.* ¶ 14.

125 *Id*. (emphasis added).

126 *Id.* ¶ 17.

127 *Id.* ¶¶ 14-17.

E. Scholarly Approaches and Proposals Regarding the Search of Fitness Trackers

Several academics have addressed the question of whether a warrant should be required to search a digital device found on an arrestee at the time of arrest.[128] Those who have undertaken the task to formulate a proposed solution have not all reached the same rule, nor have they addressed the issue on the same front. Some prefer to approach the issue in terms of a blanket warrant requirement set forth by the Supreme Court.[129] In perhaps taking notice of the Court's timelines regarding application of the Fourth Amendment to new issues, others sought resolution outside the Court, pressing for additional and rigorous regulation,[130] and some have concluded the manufacturer ought to be responsible for safeguarding the data.[131] The following provides scholars' attempts to address the issue at bar.

1. The Blanket Rule Approach

One proposed method would require law enforcement to obtain a warrant for all searches of digital devices found on a person.[132] In an application of *Riley v. California* to fitness trackers proposed in the Minnesota Law Review, the author contended, because of the bright-line rule set forth by *Riley* for cell phones, a bright-line rule should similarly exist for fitness trackers.[133] The author who proposed this rule considered fitness trackers that "tend to have a single button allowing the data to come across the screen one by one . . . ."[134]

Further, the author provides counterarguments for those who suggest that certain types of data should be protected, for instance, "allowing officers to access step count or flights of stairs climbed without a warrant."[135] In such cases, the author referred to the impracticality of an officer having to make a determination as to what information was protected and that the "physical

---

128 *See generally* Saphner, *supra* note 10; Augustine, supra note 10; Eugene R. Milhizer, *Applying the Digital Search Incident to Arrest Doctrine to Predigital Content*, 61 ST. LOUIS U. L.J. 165, 191 (2017); Jessica Kitain, *Beware of Wearables: Protecting Privacy in a Data-Collecting World*, 9 DREXEL L. REV. ONLINE 1, 25–27 (2017).

129 Saphner, *supra* note 10; *see also* Augustine *supra* note 128, at 16 ("As a result, the Pennsylvania judiciary must require law enforcement to obtain a warrant before searching wearable technology.").

130 Milhizer, *supra* note 128, at 179.

131 Kitain, *supra* note 128, at 25-26.

132 Saphner, *supra* note 10; *see also* Augustine, supra note 128, at 16 ("As a result, the Pennsylvania judiciary must require law enforcement to obtain a warrant before searching wearable technology.").

133 Saphner, *supra* note 10, at 1723.

134 *Id*.

135 *Id*.

nature of activity trackers would make such a rule even less workable[,]" because of the tendency for fitness trackers to have a single button that allows the user to see data "one by one[.]"[136] Lastly, in proposing the blanket rule, the author recognizes the exceptions set forth in *Riley*, such as exigent circumstances, which allow an officer to search a device incident to an arrest without a warrant.[137]

Another suggested type of blanket approach would require the Court to focus on the privacy interest and "be guided by enduring constitutional principles rather than the particular attributes of a transient device, however remarkable and pervasive it may be."[138] Plainly speaking, it seems the author places privacy above government interest and to solve the issue at bar, proposes a bright line ban on searches of digital devices found upon an arrestee at the time of arrest. [139]

2. Statutory Approach

Another approach proposes the U.S. Congress should enact statutes to mandate protections and allow for increased regulatory protections of fitness tracker information.[140] One author contended although fitness tracker data is not protected by HIPPA regulations, it is nevertheless "sensitive information" which should enjoy protection similar to that of HIPPA information through an adopted statute.[141] This approach calls for the U.S. Congress to take action and provide protections for the information derived from fitness trackers.[142] Although not rooted in criminal law or search incident to arrest, this approach seems to provide federally mandated protections for information derived from the fitness trackers, including how the information is shared.[143]

3. Increased Manufacturer Controls

A final approach, infused between a push for Fourth Amendment protections imposed by the Court or Congress and regulations, is examined in a Note published in the Drexel Law Review Online, which calls for the

---

136 *Id*.

137 *Id.* at 1724.

138 Milhizer, *supra* note 128, at 191.

139 *Id.*

140 Michelle M. Christovich, *Why Should We Care What Fitbit Shares?: A Proposed Statutory Solution to Protect Sensitive Personal Fitness Information*, 38 HASTINGS COMM. & ENT. L.J. 91, 112–13 (2015); *see also* Alexandra Troiano, *Wearables and Personal Health Data Putting a Premium on Your Privacy*, 82 BROOK. L. REV. 1715, 1740–41 (2017).

141 Christovich, *supra* note 140.

142 *Id.*

143 *Id.* at 112-113

manufacturers of wearables to provide users with education regarding the information derived from their wearables and for the manufacturers to strengthen privacy practices.[144] This approach seems to recognize the Court's nature and timeliness in deciding whether or not to provide protections under the Fourth Amendment and posits the correct approach is to address concerns with manufacturers.[145]

IV. CATEGORIZING FITNESS TRACKERS AND APPLYING *RILEY*—A PROPOSED RULE

The vast majority of modern cell phones are likely to fall under the protection of *Riley's* holding[146] but not all fitness trackers share common features that create a privacy concern as contemplated in *Riley*.[147] This part looks at how fitness trackers match up in comparison to other devices and items contemplated in case law, applies the *Riley* holding to fitness trackers, and proposes a rule that operates as a functional test to determine the device's capabilities thereby informing police whether or not a search may be conducted incident to an arrest. It then concludes by discussing exceptions to that rule, and responses to potential criticisms.

A. Between Smartphones, Digital Cameras, and Gift Cards, Where do Fitness Trackers Fall?

In analyzing whether a warrant is required, courts look to the object in question. In *Riley*, it was a cell phone,[148] whereas in *Turner* the object was a gift card,[149] and in other cases, an iPod[150] and a digital camera.[151] Next, the courts weigh the interest of the government against the interest of the people, while at the same time referencing the item in question and its functionality.[152]

---

144 Kitain, *supra* note 128, at 26.

145 *Id.* at 25.

146 Riley v. California, 134 S. Ct. 2473, 2480–81 (2014) (discussing that one cell phone was a flip phone and the other a smart phone).

147 *See generally* Hilmantel, *supra* note 12.

148 *See generally Riley*, 134 S. Ct. 2473 (the Court held cell phones enjoyed protections under the Fourth Amendment, and despite the general exception to the warrant requirement for searches incident to an arrest, searches of cell phones would require a warrant absent exigent circumstances).

149 United States v. Turner, 839 F.3d 429, 435–36 (5th Cir. 2016) (holding a gift card had substantially less, if any data contained on it and did not enjoy protections as contemplated under *Riley*).

150 People v. Folsom, 2017 COA 146M, ¶¶ 14-17, *as modified on denial of reh'g* (Colo. App. Dec. 28, 2017) (holding an iPod enjoyed the protections of a cell phone because of the data it was able to, and did contain).

151 *Turner*, 839 F.3d at 435–36 (holding a digital camera did not have the same features as a smart phone and therefore the holding in *Riley* did not apply).

152 *See Riley*, 134 S. Ct. at 2489; *see also Turner*, 839 F.3d at 435–36.

In analyzing fitness trackers, the Court will do the same, but a problem exists because not all fitness trackers are the same.[153] Some have the ability to provide text and call notifications, display GPS routes, and log a plethora of personal health related data, as well as run third-party applications, whereas others may simply provide the user with pedometer readouts, calories burned, distance, and time.[154]

In further assessing fitness trackers in comparison to other protected and non-protected devices, the U.S. Supreme Court, as lower courts have, may consider the memory capacity of the device.[155] For instance, a gift card contains about "2,000 to 8,000 electronic bytes of data (the equivalent of several pages of data),"[156] whereas the digital camera in *Miller* held about 2 gigabytes of data.[157] The current, most advanced Fitbit tracker, the "Ionic," holds about 2.5 gigabytes of data,[158] and a cell phone can come with 8, 16, and even 64 gigabytes of memory.[159] Based on storage capacity alone, one could conclude that fitness trackers could hold more than a gift card and digital camera, but less than a common smart phone, putting fitness trackers somewhere in the middle. On the other hand, some fitness trackers, like the FitBit "Zip," have substantially less memory capability, only capturing basic fitness tracking data for a few days and without any internal memory for music, or application software.[160]

As a result, fitness trackers may or may not contain the kind of information thought to need the added protection of a warrant. Such a determination would very well depend on the tracker's features, functionality, and memory capacity, among other things. Fitness trackers, by this logic, *could* fall somewhere below the now protected cell phone but above a gift card, both in comparison to the kind and amount of information it could contain. Because of the diversity among trackers, in comparison to cell phones, a blanket rule requiring a search warrant for *all* digital devices found on an arrestee, as proposed by other scholars, is overly broad.[161]

---

153 *See generally* Hilmantel, *supra* note 12.

154 *Id.*

155 *Turner*, 839 F.3d at 435–36*; see also* United States v. Miller, 34 F. Supp. 3d 695, 700 (E.D. Mich. 2014).

156 *Smart Card*, TECH-FAQ, http://www.tech-faq.com/smart-card.html (last visited Nov. 9, 2017).

157 *Miller*, 34 F. Supp. 3d at 700.

158 *Fitbit Ionic - Smartwatch Specifications*, *supra* note 25.

159 *Miller*, 34 F. Supp. 3d at 700.

160 FITBIT, *supra* note 17.

161 *See generally* Saphner, *supra* note 10 (noting a sweeping rule to require police to obtain a warrant prior to searching any digital device incident to an arrest).

B. Applying *Riley* to Fitness Trackers

The Court should analyze the search of fitness trackers (found on an arrestee's person) just as it did with cell phones in *Riley*.[162] In doing so, the Court would first turn to the interests of the government. The Court here would likely recognize the same government interest as it did in *Riley* in that law enforcement may preserve evidence[163] and protect themselves by conducting an examination of the outside of the fitness tracker to evaluate if it poses a danger to officer safety (such as a concealed razor blade).[164] If the officer is concerned about the device being remotely wiped, the officer could "place it in an enclosure that isolates the [fitness tracker] from radio waves."[165] Removing the device from the arrestee and placing it in a "Faraday bag" would remove concerns of evidence destruction and this could be done whether or not the device had Wi-Fi, Bluetooth, or cellular abilities.[166]

Next, in analyzing the privacy interest at stake, the Court could find a fitness tracker (again dependent on its capabilities) does have similar features that a cell phone has. Such features *could* include "both a quantitative and a qualitative" differences in comparison to the cigarette pack contemplated in *Robinson*, or other object found on an arrestee's person.[167]

Fitness trackers, much like cell phones, *can* have the ability to display video, contacts, calendars, maps, medical like data, text messages, and call log information. In *Riley*, the Court found the cell phone to have many of these features, noting they are like "minicomputers that also happen to have the capacity to be used as a telephone."[168] Likewise, a fitness tracker could be viewed in a similar light in that they are minicomputers with many functions, one of which is a pedometer.

In *Riley*, the Court also recognized a cell phone poses distinct privacy concerns in that they contain a collective of information all in one place.[169] Likewise, some (but not all) fitness trackers contain a collective amount of information that consolidate calendars, emails, call logs, medical data, text messages, GPS data, mobile payment information, and alerts from applications such as Facebook and Gmail.[170] Many fitness trackers are

---

162 *See generally* Riley v. California, 134 S. Ct. 2473 (2014).

163 *Id.* at 2486.

164 *Id.* at 2485.

165 *Id.* at 2487.

166 *Id.*

167 *Id.* at 2488–91 (discussing the privacy and safety differences as applied to the Fourth Amendment to cell phones and the search of a cigarette pack).

168 *Id.* at 2489.

169 *Id.*

170 *FitBit Ionic Watch*, *supra* note 22 (FitBit advertises, "Stay connected to what matters most with texts, calls and calendar alerts & notifications from apps like Facebook and Gmail.").

designed to work with software applications,[171] such as a cell phone and/or a computer that stores information, something also contemplated in *Riley*, with cloud computing.[172]

The *Riley* Court was also concerned with the storage capacity of modern cell phones, noting they allow people to "carry a cache" of data with them throughout the day,[173] and among that information is data that is "never found in a home in any form—unless the phone is."[174] The same could be expected with fitness trackers; however, this would not account for all trackers, as some only track steps, calories, and distance, with a feature to provide the date and time.[175] Dependent on the fitness trackers functionality, it is possible that the information on the tracker could allow "[t]he sum of an individual's private life can be reconstructed through" the cumulative data contained on the device, at least much more so than "a photograph or two of loved ones tucked into a wallet."[176]

As a result of the *Riley* application to fitness trackers, the government interest still remains virtually unfettered and concerns of officer safety and preservation of evidence can be thwarted by simple steps, even if the device is not similar to a cell phone as contemplated in *Riley*.[177] On the other hand, the privacy interest in the device varies dependent on the device itself, so a plain application of *Riley* would only yield varying results. In applying *Riley* to fitness trackers and, potentially, other wearable devices, uncertainty still exists because of the varying nature of trackers,[178] and surely a sweeping bar requiring a warrant would be too broad and counter intuitive to the Court's Fourth Amendment jurisprudence. Thus, a rule applying the *Riley* Court's reasoning to the unique features of wearable trackers must be proposed.

---

171 *Riley*, 134 S. Ct. at 2490–91 ("Mobile application software on a cell phone, or 'apps,' offer a range of tools for managing detailed information about all aspects of a person's life.") ("Such a search would be like finding a key in a suspect's pocket and arguing that it allowed law enforcement to unlock and search a house.").

172 *Id.* at 2491 ("To further complicate the scope of the privacy interests at stake, the data a user views on many modern cell phones may not in fact be stored on the device itself.").

173 *Id.* at 2489-91.

174 *Id.* at 2491.

175 FITBIT, *supra* note 17.

176 *Riley*, 134 S. Ct. at 2489.

177 *Id.* at 2485-87.

178 *See generally* Hilmantel, *supra* note 12.

C. The Proposed Rule

Not all fitness trackers fit squarely into a *Riley* application because not all fitness trackers are the same.[179] Unlike modern cell phones,[180] fitness trackers must be categorized to provide clarity for law enforcement and courts, as well as provide protections for the people without creating broad sweeping warrant requirements where they are not needed. Not all fitness trackers contain private data like a typical cell phone or even a "dumb" phone, as contemplated in *Riley*.[181] The proposed rule provided in this section splits trackers up into two main categories, those that are much like a cell phone as determined in *Riley*[182] and those that are more like the pack of cigarettes as determined in *Robinson*.[183] In short, the proposed rule allows law enforcement to inspect a device found on an arrestee for officer safety reasons, for evidence logging, and/or to make a field determination of whether the device is an "advanced" device that requires a warrant before searching or a "feature deficient" device which does not require a warrant to search.

1. How do Police Determine Which Category a Device is in?

Because of the need to allow officers to protect themselves and preserve evidence of criminal activity, as discussed in *Chimel*,[184] police are permitted to remove the device from the arrestee and conduct a cursory inspection of the watch to determine whether the watch falls under category one or two.[185] This search is limited to physically inspecting the exterior of the device for officer protection, as indicated in *Riley*.[186]

During the cursory inspection, an officer may determine which category the tracker falls under. If an officer believes a search of the tracker is required, he or she may use this cursory search to determine which category the tracker falls in, using a "totality of facts" test to determine if a warrant would be required before searching the device. If knowledge of the device is limited, a simple look at the tracker for the manufacturers name or logo along with an internet search (much like police use of reference materials to

---

179 *See generally* Hilmantel, *supra* note 12.

180 *Demographics of Mobile Device Ownership and Adoption in the U.S.*, PEW RES. CTR. (Feb. 5, 2018), http://www.pewinternet.org/fact-sheet/mobile/ (noting 95% of Americans own a cell phone, of which 77% are smart phones).

181 *See generally Riley*, 134 S. Ct. 2473.

182 *Id.* at 2488–91 (discussing the differences between cell phones and the search of a cigarette pack).

183 *Id.*

184 Chimel v. California, 395 U.S. 752, 762–63 (1969).

185 *Id*.

186 *Riley*, 134 S. Ct. at 2485.

identify pills, except less expansive and intricate) may be used to determine the tracker's features.[187]

In the end, if the arresting officer believes the device contains evidence of criminal activity or evidence of the crime of arrest but is also a "feature rich" device subject to the *Riley* exception, he or she may preserve the tracker in a "Faraday bag" or simply power off the device[188] and then seek a warrant.

2. Category One: "Feature Deficient" Fitness Trackers, No Warrant Required

In the first category, a fitness tracker that tells the time and date on a digital screen, usually easily identified by their plain solid state digital screen that gives readouts in designated places indicating the time, date, and perhaps number of steps, activity time, calories burned, would not require police to obtain a warrant to search the device.[189] These devices are not comparable to the "minicomputer" private data carrying devices contemplated in *Riley*.[190]

"Feature deficient" devices lack advanced features that create the privacy concerns contemplated in *Riley*. Therefore, they do not yield highly lucrative and private information and are much like the pack of cigarettes contemplated in *Robinson*.[191] Identification of these devices may be as simple as observing it has single color OLED display to view information or by following the category determination as described above. Upon a lawful arrest, if the device is not comparable to a cell phone with peripheral features that serve as a trove of private data, officers are free to search the device without a warrant.

3. Category Two: "Advanced" Fitness Trackers, Warrant Required, Unless Exception

The second category includes fitness trackers that have comparative features like cell phones or in the Court's analogy, "minicomputers."[192] These advanced fitness tracker functions include, but are not limited to, text and call notification and viewing, email viewing, software application accessibility, GPS tracking, banking and pay information, and Wi-Fi connectivity, among other features that go above and beyond feature

---

187 *See, e.g.*, Kim LaCapria, *Pill Identifier App Helps Cops in The Field ID Drugs*, INQUISITR (Nov. 30, 2012) https://www.inquisitr.com/420610/pill-identifier-app-helps-cops-in-the-field-id-drugs/.

188 *Riley*, 134 S. Ct. at 2487 (discussing alternative options to preserve a cell phone's data, rather than searching it on scene, allowing the protection of evidence and time to obtain a warrant).

189 FITBIT, *supra* note 17 (for examples see the Fitbit Zip, and Flex 2).

190 *Riley*, 134 S. Ct. at 2489.

191 United States v. Robinson, 414 U.S. 218, 225–26 (1973).

192 *Riley*, 134 S. Ct. at 2489 (discussing cell phone are much like minicomputers because of the information they contain and function).

deficient trackers.[193] These devices are fitness trackers, but as the Court stated about cell phones, they are "minicomputers that also happen to have the capacity to be used as a telephone," or in this case a fitness tracker.[194] To speak plainly, these devices are similar to "smart phones," with a peripheral function geared toward fitness tracking.

Another aspect of consideration is the fitness trackers storage capacity. An "advanced" fitness tracker commonly has much more internal memory to allow for computing and storage of more data, such as software applications that run email, mobile pay information, and GPS.[195] These devices also serve as a collective of information, tied together in one central location—attached to a person's wrist and travel wherever the user may go. This concern was addressed in *Riley* and should be one of the considerations an officer bears in mind. [196]

D. Good Faith Exception and Exigent Circumstances

The Supreme Court has long recognized exceptions to warrant requirements in many different situations. As the Court in *Riley* held, some warrantless searches may be allowed under "other case-specific exceptions," such as when police are compelled by exigent circumstances.[197] Exceptions may also include a "good faith" exception,[198] or an exception for border searches.[199]

1. "Good Faith" Exception

An exception that should apply here is the "good faith" exception, similar to the rule contemplated in *Herring v. United States*.[200] Police conducting a search in objectively "good faith" would not be categorical cause for excluding evidence unless such conduct by police was "sufficiently deliberate that exclusion can meaningfully deter it, and sufficiently culpable that such deterrence is worth the price paid by the justice system."[201] Here, if a police officer conducts a search in objectively "good faith," not in "deliberate, reckless, or grossly negligent conduct, or in some circumstances

---

193 FITBIT, *supra* note 17 (for examples see the Ionic, and Charge 2).
194 *Riley*, 134 S. Ct. at 2489.
195 FITBIT, *supra* note 17 (for examples see the Ionic in comparison to Zip models).
196 *Riley*, 134 S. Ct. at 2489-90.
197 *Id.* at 2494.
198 *See generally* Herring v. United States, 555 U.S. 135, 144 (2009).
199 *See generally* United States v. Saboonchi, 48 F. Supp. 3d 815, 817–20 (D. Md. 2014).
200 *See generally Herring*, 555 U.S. at 144.
201 *Id.*

recurring or systemic negligence," the data recovered would be valid evidence.[202]

As an example, if a police officer took steps to determine which of the two categories the device fit under and later found that he made an error in doing so and as a result conducted a search of a tracker that would have otherwise required police to obtain a warrant, the evidence derived from such a search is not categorically inadmissible. Instead, the evidence could be subject to an objective standard review as to whether the officer's conduct was objectively in "good faith." The exception here, as it would be applied, would allow for police to use objective judgment in determining if a device is "feature deficient" that may be searched without a warrant, or an "advanced" fitness tracker where police must first obtain a warrant.

2. Exigent Circumstances

In *Riley*, the U.S. Supreme Court recognized there would be instances wherein law enforcement would have a valid reason to forego a warrant and conduct a search; one such reason is exigent circumstances.[203] Such exigency may exist when police determine the threat of death or serious bodily harm is imminent, when officer safety is in imminent danger, or when destruction of evidence is imminent.[204] However, the Court has determined such an exception is reviewed in a fact specific, case-by-case basis.[205]

E. Responses to Potential Criticism of the Proposed Rule

Critics of this proposed rule may fear its complexity and protective value in comparison to a sweeping ban on searches of digital devices found on an arrestee. However, this concern is misplaced once Fourth Amendment jurisprudence is applied and thought is given to the effects a bright line ban creates. In this section, these two-overarching criticisms are addressed in turn.

---

202 *Id.*
203 Riley v. California, 134 S. Ct. 2473, 2486 (2014).
204 *Id.* at 2494.
205 *Id.* at 2486.

1. The Proposed Rule Balances Government Interest and Private Interest Correctly

Bright line rules can provide clarity[206] but risk being overly broad. A bright line rule would remove the need for analysis based on device characteristics (such as the analysis in *Riley*), but when technology advances a little further, the bright line rule would likely become even more overly broad or narrow. Should the bright line ban become too broad or narrow, the Court would be forced to overrule or further mold the bright line rule (causing its own complexity beyond making categories). In the meantime, the people and law enforcement would be stuck in that misaligned rule. Making a simple field determination, based on an objective standard, allows for the proper application of warrant requirements without overstepping the government need while protecting the privacy interest contemplated in *Riley*.[207]

2. The Proposed Rule does not Further Confusion among Law Enforcement

One potential criticism is that in creating categories, it would require law enforcement to make field determinations as to whether a device requires a warrant be obtained to search it if found on an arrestee. Such an argument is misplaced and may indicate that some advocates for these strict protections may be disconnected from the prudential nature of the Court's Fourth Amendment jurisprudence, as the Court has not favored these sweeping bans and brash guillotine cuts of Fourth Amendment related activity when there is a valid government interest at stake.[208]

Those who criticize the proposed rule on the basis of creating more complexity and confusion for law enforcement may overlook the discretion and faith the Court affords to law enforcement in making determinations in the field. Police officers already make determinations of great weight in the field, such as the decision to conduct an inventory search or open a

---

206 *See, e.g.*, Thornton v. United States, 541 U.S. 615, 619-20 (2004) (the Court discusses its holdings from previous cases, using words like "workable rule," and "clear rule for police and citizens alike.").

207 *Riley*, 134 S. Ct. at 2489-91.

208 *See, e.g.*, Chimel v. California, 395 U.S. 752, 764–65 (1969) (the Court rejected a rule proposal that would allow a search of a person entire home, so long he was arrested in it, stating if such a rule were valid the Fourth Amendment would near a "evaporation point.").

container[209] or whether to use deadly force[210] and so on. Determining whether a fitness tracker fits within the scope of *Riley's* holding (as an "advanced" fitness tracker) asks no more of an officer's ability or discretion. The identification of a fitness tracker is not in practice a life or death determination, and law enforcement will have time to identify whether the device is an "advanced" or a "feature deficient" device. Nevertheless, it is important to note the Fourth Amendment does *not* demand perfection from police but does allow for police to act within reason, and "the text of the Fourth Amendment indicates, the ultimate measure of the constitutionality of a governmental search is 'reasonableness.'"[211]

V. CONCLUSION

There is a growing use of fitness trackers.[212] They are diverse in capability and kind[213] and continue to expand in functionality and data capacity.[214] Applying a functional rule based on specific category sets may prevent over or under inclusion of devices and provide law enforcement the ability to search devices that fall short of the rule announced in *Riley*.[215] A functional rule will also allow protections of the ever-growing sensitive information that people carry on their persons in their daily activities. This rule could create confusion for law enforcement in making distinctions in a device's capability, however, given the already high number of users of these devices,[216] and the reasonably easy identifiable nature of a fitness tracker, the

---

209 Florida v. Wells, 495 U.S. 1, 4 (1990) ("A police officer may be allowed sufficient latitude to determine whether a particular container should or should not be opened in light of the nature of the search and characteristics of the container itself. Thus, while policies of opening all containers or of opening no containers are unquestionably permissible, it would be equally permissible, for example, to allow the opening of closed containers whose contents officers determine they are unable to ascertain from examining the containers' exteriors. The allowance of the exercise of judgment based on concerns related to the purposes of an inventory search does not violate the Fourth Amendment.").

210 Graham v. Connor, 490 U.S. 386, 396-97 (U.S. 1989) ("The calculus of reasonableness must embody allowance for the fact that police officers are often forced to make split-second judgments—in circumstances that are tense, uncertain, and rapidly evolving—about the amount of force that is necessary in a particular situation.").

211 Vernonia Sch. Dist. 47J v. Acton, 515 U.S. 646, 652 (1995).

212 FITBIT, *supra* note 16.

213 *See generally* Hilmantel, *supra* note 12.

214 *See generally* Jill Duffy & Alex Colon, *The Best Fitness Trackers of 2017*, PCMAG (Oct. 2, 2017, 1:43 PM), https://www.pcmag.com/article2/0,2817,2404445,00.asp (discussing various uses, and features of fitness trackers available in 2017).

215 *See generally* Riley v. California, 134 S. Ct. 2473 (2014) (the Court held cell phones enjoyed protections under the Fourth Amendment, and despite the general exception to the warrant requirement for searches incident to an arrest, searches of cell phones would require a warrant absent exigent circumstances).

216 Graziano, *supra* note 13 (citing information provided by International Data Corporation) (noting device sales of 102.4 million in 2016).

application should not pose any more difficulty in application than any other determination law enforcement officers are called to make daily.[217]

As the scenario posed in the beginning, a suspect asserted a categorical ban on searches of *all* digital devices in order to prevent his sleep data from being used by the prosecution. Such a sweeping ban could allow the suspect to walk despite his actual guilt, thus disregarding the government interest in the search of the tracker. Likewise, allowing the government free reign outside of *Riley's* cellphones is not in the best interest of privacy for the people. Application of this functional rule keeps the door open for valid government interest and protects the privacy of the people. Lastly, such application should be a leap forward in protections for the people and clarity for police in contrast to the current state of the law, all while maintaining a proper judicial role and paying prudential and doctrinal respect to the Fourth Amendment without "outrunning it."

---

[217] *See generally* Graham v. Connor, 490 U.S. 386, 396-97 (U.S. 1989); *see also* Florida v. Wells, 495 U.S. 1, 4 (1990).