Note

You Should Be Free To Talk the Talk and Walk the Walk: Applying *Riley v. California* to Smart Activity Trackers

Katharine Saphner∗

Are you one of the millions of Americans tracking their bodily movements with a smart activity tracker produced by Fitbit, Jawbone, Nike, or their competitors?[1] These activity trackers come in a variety of forms, such as wristbands,[2] clip-on devices,[3] shoe inserts,[4] and shirts.[5] They collect data on steps

∗ J.D. Candidate 2016, University of Minnesota Law School; B.A. 2013, University of Minnesota. I would first and foremost like to extend my thanks to the many teachers and professors who critiqued and strengthened my writing over the years, with special thanks to Professor Joel Samaha, whose spirited lectures impressed upon me the importance of criminal procedure. Thank you also to my family, especially my parents Dan and Ethel Saphner, for instilling in me the value of hard work and persistence. Additional thanks to Robert Krizmanic, Winter Kucharski, Rachel Thrasher, Bronwyn Deen, Sheewin Pananookooln, and Emily Pribnow who provided unending patience, emotional support, and encouragement through the process of producing this Note and my law school career. Finally, my heartfelt thanks to Professor JaneAnne Murray for her thoughtful input and feedback on this Note and to the staff and board of the *Minnesota Law Review*, especially Anna Luczkow, Olivia Moe, Julia Glen, Jon Finch, and Jerry Kerska, for carrying this Note to publication with their careful edits.

1. Tony Danova, *Just 3.3 Million Fitness Trackers Were Sold in the US in the Past Year*, BUS. INSIDER (May 5, 2014, 4:22 PM), http://www.businessinsider.com/33-million-fitness-trackers-were-sold-in-the-us-in-the-past-year-2014-5 (indicating that 3.3 million activity trackers were sold between April 2013 and March 2014).

2. *See, e.g.*, *Flex*, FITBIT, https://www.fitbit.com/flex (last visited Mar. 7, 2016); *Nike + Fuelband*, NIKE, https://secure-nikeplus.nike.com/plus/products/fuelband (last visited Mar. 7, 2016); *Up*, JAWBONE, https://jawbone.com/up (last visited Mar. 7, 2016).

3. *See, e.g.*, *One*, FITBIT, https://www.fitbit.com/one (last visited Mar. 7, 2016); *Zip*, FITBIT, https://www.fitbit.com/zip (last visited Mar. 7, 2016).

4. *See, e.g.*, Alice Truong, *Forget Clip-on Trackers and Wristbands: This Smart Shoe Insole Will Track Your Physical Activity*, FASTCOMPANY (Apr. 15, 2014, 8:27 AM), http://www.fastcompany.com/3029051/world-changing-ideas/forget-clip-on-trackers-and-wristbands-this-smart-shoe-insole-will-trac (describing a smart sole insert created by SmartMove).

taken,[6] flights of stairs climbed,[7] calories burned,[8] efficiency of sleep,[9] GPS location,[10] and heart rate and respiratory activity.[11] If you are an activity tracker user, perhaps you bought your tracker in an effort to stay on top of your health, or maybe your employer gave it to you as part of a workplace health initiative.[12] Now suppose that you are arrested. As the arresting officer pats you down to search for weapons, he finds the Fitbit Charge HR[13] on your wrist. May the officer lawfully toggle through your daily fitness statistics without a warrant?

As time passes, this question becomes more pressing. American society has embraced wearable technology. Smart activity trackers are becoming more ubiquitous each year, with sales increasing 500% annually over the last several years,[14] and further growth expected in the future.[15] Wearers indicate that when these trackers are worn all day, every day, they cease to feel like an accessory; they become an extension of the

5. *See, e.g.*, Robert Vamosi, *Hexoskin's On a Mission To Change Personal Health Management*, FORBES (Oct. 10, 2014, 12:29 PM), http://www.forbes.com/sites/robertvamosi/2014/10/10/hexoskins-on-a-mission-to-change-personal-health-management (discussing clothing that collects health data); *Hexoskin Wearable Body Metrics*, HEXOSKIN, http://www.hexoskin.com (last visited Mar. 7, 2016).

6. *See, e.g.*, *Flex*, *supra* note 2; *One*, *supra* note 3; *Up*, *supra* note 2; *Zip*, *supra* note 3.

7. *See, e.g.*, *Flex*, *supra* note 2; *One*, *supra* note 3.

8. *See, e.g.*, *Flex*, *supra* note 2; *One*, *supra* note 3.

9. *See, e.g.*, *Flex*, *supra* note 2; *One*, *supra* note 3; *Up*, *supra* note 2.

10. *See, e.g.*, *Forerunner® 10*, GARMIN, https://buy.garmin.com/en-US/US/into-sports/running/forerunner-10/prod107143.html (last visited Mar. 7, 2016); *Surge*, FITBIT, http://www.fitbit.com/surge (last visited Mar. 7, 2016).

11. *Charge HR*, FITBIT, https://www.fitbit.com/chargehr (last visited Mar. 7, 2016); *Fitbit Blaze*, FITBIT, https://www.fitbit.com/blaze (last visited Mar. 7, 2016); Vamosi, *supra* note 5.

12. Employers seeking to increase productivity and decrease healthcare costs see activity trackers as "quick wins." Andrea Davis, *Wearable Devices: Future of Wellness or Just a Fad?*, EMP. BENEFIT NEWS (Oct. 9, 2014, 9:31 AM), http://ebn.benefitnews.com/news/ebn_hc_wellness_disease/wearable-devices-just-a-fad-or-the-future-of-wellness-2744272-1.html.

13. *Charge HR*, *supra* note 11.

14. Danova, *supra* note 1 (providing statistics on wearable fitness tracker sales).

15. *See Worldwide Wearable Computing Market Gains Momentum with Shipments Reaching 19.2 Million in 2014 and Climbing to Nearly 112 Million in 2018, Says IDC*, BUSINESS WIRE (Apr. 10, 2014, 8:30 AM), http://www.businesswire.com/news/home/20140410005050/en/Worldwide-Wearable-Computing-Market-Gains-Momentum-Shipments [hereinafter *Worldwide Wearable Computing Market*] (predicting that activity trackers will lead the wearable tech market through 2018).

wearer,[16] forged by a kinship very similar to that attachment most individuals feel to their engagement rings or to their cell phones. These trackers become the silent, ever-present witness to the lives of their wearers. The data contained on these devices can therefore be indescribably helpful in police investigations in which there are no objective impartial witnesses. In June of 2015, the data contained in a Fitbit device helped law enforcement officers determine that a purported rape victim had not been sleeping in her bed at the time of the alleged rape as she had claimed, but was in fact walking around her apartment.[17] The Fitbit data was used not only to discredit her claim, but also as evidence to support the woman's eventual prosecution. Activity trackers are increasingly prevalent, and contain a large quantity of intimately personal data that carries huge potential to aid in law enforcement investigations. However, courts and scholars have yet to consider whether a suspect's activity tracker may be searched without a warrant incident to the suspect's arrest.

To confront this issue, courts must determine the lasting power of a leading Supreme Court case that has long governed container searches in the wake of a recent case establishing an exception of indeterminate breadth. In *United States v. Robinson*, the Court ruled that a container found on Robinson's person during an arrest—a crumpled package of cigarettes—could be searched without a warrant at the time of his arrest.[18] However, the Court recently held in *Riley v. California* that *Robinson* does not apply to cell phones.[19] Officers are therefore required to obtain a search warrant before conducting a search of

16. *See, e.g.*, Sara M. Watson, *Stepping Down: Rethinking the Fitness Tracker*, ATLANTIC (Sept. 25, 2014), http://www.theatlantic.com/technology/archive/2014/09/hacking-the-fitness-tracker-to-move-less-not-more/380742 (claiming that the author's Fitbit was an "extension of [her] awareness of distance, of quantified movement through space").

17. Mariella Moon, *Fitbit Tracking Data Comes Up in Another Court Case*, ENGADGET (June 28, 2015), http://www.engadget.com/2015/06/28/fitbit-data-used-by-police ("The woman told the police she woke up around midnight with the stranger on top of her, and that she lost her tracker while struggling against her assailant. However, authorities found her Fitbit, which recorded her as active, awake and walking around all night."); *see also* Lynnsey Gardner, *Fitness Tracker Data Used in Court Cases*, NEWS4JAX (Feb. 22, 2016, 11:29 PM) http://www.news4jax.com/news/investigations/fitness-tracker-data-now-used-as-evidence-in-court-cases ("Police believe the steps recorded on her device prove Nina was awake and staging the crime scene instead of being asleep and ripped out of bed like she claimed.").

18. 414 U.S. 218, 236 (1973).

19. 134 S. Ct. 2473, 2485 (2014).

a cell phone at the time of the suspect's arrest.[20] The *Riley* Court relied on the storage capacity and ubiquity of modern cell phones,[21] but much of its analysis is arguably applicable to all digital data, whether or not it is found on a cell phone.[22] Courts have just begun to flesh out the contours of the *Riley* exception, and must determine how to apply *Riley* to other digital containers, including increasingly popular smart activity trackers. Smart activity trackers are just one type of digital device that courts will have to face. In the not-so-distant future, it is probable that numerous types of personal data will be collected and stored on devices individuals use and carry with us at all times. For this reason, it is crucial that courts apply *Riley* consistently to the myriad of smart devices on the market.

This Note argues that courts should interpret *Riley* as proscribing unwarranted searches of all digital data on smart devices found on the persons of arrestees, including smart activity trackers. Part I describes the Court's treatment of arrest searches and searches of digital data, the Court's protection against certain types of unwarranted searches, and the increasing popularity and capacity of smart activity trackers. Part II analyzes the position of smart activity trackers in relation to other wearable smart technology previously governed by *Robinson* and recently contemplated by *Riley*, and discusses the need for practical and workable law enforcement rules. Part III concludes that courts should interpret *Riley* as endorsing a two-tiered approach that carefully distinguishes warrantless searches of physical items from searches of the digital data they contain, allowing the former but prohibiting the latter. Ultimately, this Note argues that law enforcement officers should be allowed to physically search smart devices without a warrant, but should be required to obtain warrants to search digital data on smart activity trackers, and encourages further officer education regarding the types of devices available.

I. FOURTH AMENDMENT JURISPRUDENCE HAS BEEN INCREASINGLY PROTECTIVE AGAINST HIGH-TECH GOVERNMENT INTRUSION

Though Fourth Amendment protections have advanced in recent years, it is not yet clear how smart activity trackers—or

20. *Id.*

21. *Id.* at 2489–91.

22. *See, e.g.*, *id.* at 2485 ("No [security-based] unknowns exist with respect to digital data.").

other smart devices—will be treated by officers conducting searches incident to arrest. This Part first describes the purpose of the Fourth Amendment and introduces broad constitutional search requirements, and then provides a primer on existing case law that serves as the legal backdrop for law enenforcement searches of smart data. Finally, this Part explores the growing smart activity tracker trend in greater depth, demonstrating the criminal justice system's need for a definitive placement of smart activity trackers within the Fourth Amendment framework.

A. THE FOURTH AMENDMENT'S PROTECTIONS AGAINST UNREASONABLE SEARCHES

The Fourth Amendment guarantees Americans the right "to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures."[23] The Founders wrote and adopted the Fourth Amendment specifically to protect against excessively probing searches by the government, policing the boundary between necessary government intrusion and personal privacy.[24] The Founders specifically aimed to protect not only physical objects, but private information as well, and therefore included a specific protection of "papers."[25] The Court has further emphasized the focus on protecting intangible aspects of its citizens' lives from government intrusion by finding that the government seizes property by meaningfully interfering with an individual's possessory property interests and that it conducts a search when it infringes upon expectations of privacy that society considers reasonable.[26]

The Supreme Court has often analyzed Fourth Amendment requirements and has laid out guidelines for lower courts and law enforcement agencies regarding its parameters. The

23. U.S. CONST. amend. IV. The amendment also states that "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." *Id.*

24. *See* Thomas K. Clancy, *The Fourth Amendment's Concept of Reasonableness*, 2004 UTAH L. REV. 977, 980–84 (describing the use of suspicionless searches in the era just before the revolutionary war and the backlash in the American colonies influencing the Framers).

25. Brief for the Cato Institute as Amicus Curiae Supporting Petitioner at 11, *Riley*, 134 S. Ct. 2473 (No. 13-132) (noting that the Framers "used written communications, both public and private, to revolutionize political life on the American continent, so they promptly provided for protection of information against government seizure and search after the founding").

26. *See* United States v. Jacobsen, 466 U.S. 109, 113 (1984).

Court has generally required officers to obtain search warrants prior to searching, so inferences supporting the search will be assessed by a neutral judge and not only by the potentially biased officer.[27] However, if the search falls under one of the warrant requirement's many established exceptions,[28] no warrant is necessary.[29] Exceptions to the warrant requirement are established by balancing the degree of intrusion on the defendant's privacy with the degree to which the exception is needed to promote government interests.[30]

One exception to the warrant requirement is the exigent circumstances requirement, which allows law enforcement officers to perform warrantless searches in emergency circumstances: "[t]he 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."[31] Another exception allows officers to conduct searches incident to lawful arrests—searching both the arrestee's person[32] and the area within the arrestee's control.[33] Though the exact scope of the legally searchable area has changed over time, the Court has never cast doubt on the premise that at a minimum the arrestee's person may be searched.[34] Two discrete justifications support the search incident to a lawful arrest exception.[35] First, courts have long held that officers may search for and seize weapons to maintain their own safety.[36] Second, courts allow

27. *See Riley*, 134 S. Ct. at 2482.

28. *See, e.g.*, Benjamin T. Clark, *Why the Airport and Courthouse Exceptions to the Search Warrant Requirement Should Be Extended to Sporting Events*, 40 VAL. U. L. REV. 707, 715 (2006) (listing many exceptions, including consent, stop and frisk, airports, courthouses, hot pursuit, borders, searches incident to arrest, and drug testing of high school athletes).

29. *See Riley*, 134 S. Ct. at 2482.

30. *See* Wyoming v. Houghton, 526 U.S. 295, 300 (1999) (discussing the balancing required for exceptions to the warrant requirement).

31. Warden, Md. Penitentiary v. Hayden, 387 U.S. 294, 298–99 (1967).

32. Weeks v. United States, 232 U.S. 383, 392 (1914) (noting that the government's right "to search the person of the accused when legally arrested . . . has been uniformly maintained in many cases").

33. United States v. Robinson, 414 U.S. 218, 224 (1973).

34. *See id.* at 225–26 (citing a string of authorities supporting the proposition).

35. *See* Chimel v. California, 395 U.S. 752, 762–63 (1969) (detailing the justifications for exceptions).

36. *See Robinson*, 414 U.S. at 231 ("A due regard for [the officer's and the public's] safety . . . justif[ies] a sufficient search to ascertain if such weapons were carried about the person . . . and . . . to seize and hold them." (quoting Closson v. Morrison, 47 N.H. 482 (1867))).

officers to seize evidence of the crime to ensure its preservation.[37] *Chimel v. California* laid down the first limitations on searches incident to arrest, holding a warrantless search of an entire home is unreasonable, but searching areas in the immediate control of an arrestee is reasonable,[38] a holding later extended to searches of the persons of arrestees.[39]

B. THE COURT'S TREATMENT OF WARRANTLESS SEARCHES PRIOR TO *RILEY*

In *United States v. Robinson* and its progeny, the Court applied *Chimel*'s rationale to the context of police pat downs.[40] This Section describes the decisions that led to the warrant requirements as they existed at the time the Court considered *Riley*. This Section then describes the Court's protective treatment of advanced technology in the search context.

1. *United States v. Robinson* Enables Constitutional Container Searches

The *Robinson* Court applied *Chimel* to the search of a container found on an arrestee's person.[41] An officer pulled over Robinson on suspicion of driving without a license, informed him he was under arrest, and upon patting him down, "felt an object in the left breast pocket of the heavy coat [Robinson] was wearing."[42] The officer reached into the pocket and pulled out an object that appeared to be a "crumpled up cigarette package."[43] Feeling objects inside the package, the officer opened it, finding fourteen capsules filled with heroin.[44]

Robinson holds that neither the search nor seizure of the items violated the Fourth Amendment.[45] Though the opinion notes that the arresting officer could not tell what the object

37. *See id.* at 230 ("[C]ustody is of no value if the law is powerless to prevent the abstraction or destruction of this evidence, without which a trial would be no more than an empty form." (citing Dillon v. O'Brien [1887] 16 Cox Crim. Cas. 245 (Exch. Div.) (Ir.))).

38. 395 U.S. at 762–63.

39. *See Robinson*, 414 U.S. at 224.

40. *See id.*

41. Riley v. California, 134 S. Ct. 2473, 2488 (2014). In fact, *Robinson* was the only case to apply *Chimel* to the search incident to lawful arrest until *Riley*. *Id.*; *see Robinson*, 414 U.S. at 257–59 (applying *Chimel*).

42. *Robinson*, 414 U.S. at 220–23.

43. *Id.* at 223.

44. *Id.*

45. *Id.* at 224.

was, and once he held the package in his hand, could not tell what was inside,[46] the opinion notably does not address the search of the cigarette package as separate from the search of Robinson's person.[47] Instead *Robinson* simply states that, having found the package during a lawful search, the officer was entitled to search it.[48] The dissent points out that the search of the package did not further the protective purposes for which the search began, as the cigarette package was out of the hands of the arrestee, and therefore suggested "the mere fact of an arrest should be no justification, in and of itself, for invading the privacy of the individual's personal effects."[49]

In *Robinson*, the justification for allowing warrantless searches incident to arrest "rests quite as much on the need to disarm the suspect in order to take him into custody as it does on the need to preserve evidence on his person for later use at trial."[50] Therefore, standards should not be stricter if it is unlikely that evidence of the crime will be found on the arrestee's person or there is no greater probability of weaponry being found on the person of the arrestee.[51] *Robinson* favors a categorical rule because law enforcement officer decisions as to how to search arrestees are "necessarily . . . *ad hoc* judgment[s]" and, regardless of the crime in question, arrests expose officers to similar levels of danger, so the Court opted to "treat[] all custodial arrests alike for purposes of search justification."[52]

Justice Marshall's dissent in *Robinson* spells out several concerning outcomes that could flow from *Robinson*'s holding, including the potential for officer searches of wallets and sealed envelopes found on the person of an arrestee on the basis that they might contain razor blades or pins.[53] The Court addressed several of these concerns in later cases by narrowing *Robinson*'s scope. It first addressed exactly what may be searched at

46. *Id.* at 223.

47. *See id.* at 250 (Marshall, J., dissenting) (breaking the search into three discrete stages).

48. *See* Riley v. California, 134 S. Ct. 2473, 2484 (2014); *Robinson*, 414 U.S. at 236; *see also id.* at 255–56 (Marshall, J., dissenting) ("The majority . . . fails to recognize that the search . . . included a separate search of effects found on [the defendant's] person. . . . [T]here was no justification . . . which would authorize [the officer] opening the package and looking inside.").

49. *Robinson*, 414 U.S. at 256–57 (Marshall, J., dissenting).

50. *Id.* at 234 (majority opinion).

51. *Id.* at 234–35.

52. *Id.* at 235.

53. *Id.* at 257 (Marshall, J., dissenting).

the time of arrest without a search warrant, recognizing a more distinct line between the search of an individual's person and his effects. In *United States v. Chadwick*, officers searched luggage that was seized at the time and place of the defendant's arrest, but was not searched until several hours later, when it was no longer in the control of the arrestee.[54] *Chadwick* limits the *Robinson* warrant exception to "personal property . . . immediately associated with the person of the arrestee."[55] *Knowles v. Iowa* further narrows *Robinson*'s scope, holding the doctrine inapplicable to law enforcement interactions involving only the issuance of citations.[56] *Knowles* reasons that both *Chimel* justifications are weaker when an officer issues a citation than when she arrests a suspect—in citation issuances, officer safety is not implicated to the same degree and there is no inculpatory evidence to destroy.[57] However, due to unique circumstances in the vehicle context, *Arizona v. Gant* concludes that upon arrest, officers may only warrantlessly search the vehicle of the arrestee if "the arrestee is unsecured and within reaching distance" of the searched areas or if the officer reasonably thinks that the vehicle holds evidence relevant to the crime.[58]

2. The Court's Increased Protections Against High-Tech Searches

In recent years, the Court has extended Fourth Amendment protection to cover high-tech government searches. This Subsection addresses areas of particular concern for the Court. First, this Subsection addresses the Court's protection of activities in the home from prying government eyes and its desire to protect GPS data. This Subsection goes on to discuss the Court's unwillingness to protect items that have been shared with third parties.

a. *Protection of Information Concerning the Confines of the Home*

In *Kyllo v. United States*, the Court considered whether a search subject to Fourth Amendment protections occurred

54. 433 U.S. 1, 4 (1977).

55. *Id.* at 15.

56. 525 U.S. 113, 118–19 (1998).

57. *Id.* at 116, 118–19.

58. 556 U.S. 332, 343 (2009) (noting that the exception was not implicated by *Chimel* but is needed due to unique circumstances present in automobile searches).

when police officers viewed the outside of a home with a thermal imaging device to confirm the locations of high intensity lamps that facilitate indoor marijuana growth.[59] *Kyllo* distinguishes the use of thermal imaging technology from ordinary visual surveillance, noting that officers gained "information regarding the interior of the home," which ordinarily would require physical intrusion.[60] Despite the crude system used in the case itself, *Kyllo* indicates a desire to safeguard against advanced systems, instead of "leav[ing] the homeowner at the mercy of advancing technology."[61]

Kyllo places particular emphasis on protecting the privacy of citizens, indicating that protection should depend not on the level of technology employed but on whether it enabled officer observation of intimate activity.[62] However, *Kyllo* rejects the government's suggestion that *only* "intimate" details need to be protected, saying that officers could not "know *in advance* whether . . . surveillance picks up 'intimate' details" and therefore could not determine on the spot whether surveillance would be constitutional.[63] In the home, "*all* details are intimate details" to be kept "safe from prying government eyes."[64]

Kyllo demonstrates the Court's willingness to consider law enforcement use of technology to reconstruct activities within the home as a search requiring a warrant, even where the officers did not physically enter the home.[65] Though *Kyllo* focuses on intimate details, it goes further than finding a search occurred only where private information is actually discovered. It instead concludes that where officers use a device not in public use to gather "details of the home that would previously have been unknowable without physical intrusion, the surveillance is a 'search' and is presumptively unreasonable without a warrant."[66]

59. 533 U.S. 27, 29 (2001).

60. *Id.* at 32, 34. The Court found it to be a search where the technology is not in general public use. *Id.* at 40.

61. *Id.* at 35, 36 ("While the technology [here] was relatively crude, the rule we adopt must take account of more sophisticated systems that are already in use or in development." (footnote omitted)).

62. *Id.* at 38 (noting that even low-tech systems could determine "at what hour each night the lady of the house takes her daily sauna" while a more sensitive system would be able to pick up the less intimate details such as whether or not a closet light was left on).

63. *Id.* at 39.

64. *Id.* at 37.

65. *See id.* at 41–42 (Stevens, J., dissenting).

66. *Id.* at 39–40 (majority opinion). The Court found discerning activity

b. Court Consideration of Searches Yielding Locational Data

In *United States v. Jones*, the Court again demonstrated its concern for citizen privacy when determining that the warrantless placement of a GPS device on a person's vehicle was a search in violation of the Fourth Amendment as "[t]he Government physically occupied private property for the purpose of obtaining information."[67] The Court had twice before held that gathering data from location tracking devices did not violate the Fourth Amendment,[68] but *Jones* holds that placing a GPS tracker on a vehicle is a search because it is a physical trespass.[69]

Some courts also note the unique quantity and quality of GPS data. First, this type of data produces vast stores of information but requires the use of very few resources by officers,[70] who can therefore gain a great deal of personal information about a suspect with very little effort or expense. Additionally, courts note that this data can be very personal:

> Disclosed in the data . . . will be trips the indisputably private nature of which takes little imagination to conjure: trips to the psychiatrist, the plastic surgeon, the abortion clinic, the AIDS treatment center, the strip club, the criminal defense attorney, the by-the-hour motel, the union meeting, the mosque, synagogue or church, the gay bar and on and on. What the technology yields and records with breathtaking quality and quantity is a highly detailed profile, not simply of where we go, but by easy inference, of our associations—political, religious, amicable and amorous, to name only a few—and of the pattern of our professional and avocational pursuits.[71]

Justice Sotomayor's *Jones* concurrence indicated that the government keeps this data forever and can "ascertain, more or less at will . . . political and religious beliefs, sexual habits, and

within the home requires a warrant, even with no physical intrusion into the home. *See id.* at 42 (Stevens, J., dissenting).

67. 132 S. Ct. 945, 949 (2012).

68. *See* United States v. Karo, 468 U.S. 705, 713–19 (1984) (holding a procedure similar to *United States v. Knotts* did not constitute a violation because the owner consented to the transmitter's insertion); United States v. Knotts, 460 U.S. 276, 284–85 (1983) (holding the placement of a radio transmitter in a package the defendant later received was not a Fourth Amendment violation).

69. *See Jones*, 132 S. Ct. at 949.

70. *See id.* at 963–64 (Alito, J., concurring) (indicating it "would have required a large team of agents, multiple vehicles, and perhaps aerial assistance").

71. People v. Weaver, 909 N.E.2d 1195, 1199–200 (N.Y. 2009); *see Jones*, 132 S. Ct. at 955 (Sotomayor, J., concurring) (citing *Weaver*, 909 N.E.2d at 1199).

so on," and suggested this may have an undesirable chilling effect on personal freedoms.[72]

c. Items Shared with Third Parties Typically Receive No Fourth Amendment Protection

Though it has not directly addressed the issue in the context of advanced technology, the Court held in *California v. Greenwood* that citizens have no reasonable expectation of privacy in items shared with third parties.[73] The Court found that a search of trash did not violate the Fourth Amendment because "respondents exposed their garbage to the public sufficiently to defeat their claim to Fourth Amendment protection."[74] *Greenwood* holds that even when not given to a third party, "[i]t is common knowledge that plastic garbage bags left on or at the side of a public street are readily accessible to animals, children, scavengers, snoops, and other members of the public."[75] *Jones* therefore determined that "what a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection."[76] In her *Jones* concurrence, however, Justice Sotomayor suggests that the third party information standard should be readdressed in light of the digital age.[77]

C. *RILEY V. CALIFORNIA*

The Court further expanded its protection of high-tech data in *Riley*, which lower courts are just beginning to apply. In *Riley v. California* and its companion case, *United States v. Wurie*, the Court considered whether law enforcement officers may search a cell phone found on an arrestee's person without a warrant.[78] During a pat down following Riley's arrest for firearm possession, the officer found items indicating gang affiliation and a cell phone that had many features "based on advanced computing capability, large storage capacity, and Internet connectivity."[79] The officer proceeded to access information on the phone, finding further indicia of gang involve-

72. *Jones*, 132 S. Ct. at 956 (Sotomayor, J., concurring).
73. 486 U.S. 35, 39–42 (1988).
74. *Id.* at 40.
75. *Id.* (footnotes omitted).
76. Katz v. United States, 389 U.S. 347, 351 (1967).
77. *See Jones*, 132 S. Ct. at 957 (Sotomayor, J., concurring).
78. Riley v. California, 134 S. Ct. 2473, 2480 (2014).
79. *Id.*

ment.[80] A gang crimes detective found videos of men fighting and yelling a gang name, and photos of Riley with a car police believed to be involved in a recent shooting.[81] Riley was charged with offenses related to the past shooting with an aggravating factor of benefiting a street gang, and was convicted on all counts.[82]

Riley holds that "*Robinson*'s categorical rule . . . [is] appropriate . . . in the context of physical objects," but further holds that *Robinson*'s justifications do not apply to digital data found on cell phones.[83] *Riley* detects little risk of potential harm to arresting officers, but nonetheless holds that an officer's inspection of the physical contours of the device is permissible.[84] Such a search would enable an officer to determine that the object is a cell phone rather than a bomb, and that there are no razor blades between the case and the phone, without violating the Constitution. The other justification—the avoidance of destruction of evidence—does not apply, as once the phone has been seized, the arrestee cannot destroy the phone or data within it.[85] According to the Court, the potential to avoid passcode encryption does not justify warrantless police searches of cell phones across the board. Police officers very seldom come across unlocked cell phones, and even when they do, they generally cannot conduct full searches before a data wipe occurs or the phone locks itself.[86] The Court states that to avoid as much loss of evidence as possible, officers may constitutionally disable the phone's automatic-lock feature to prevent loss of data access.[87] Finally, the Court states that privacy interests at

80. *Id.* (indicating that the arresting officer noticed some of the contacts on the phone were preceded by letters indicating gang affiliation, corresponding to other items found on Riley's person).

81. *Id.* at 2480–81.

82. *Id.* at 2481 (indicating that gang association can carry an enhanced sentence).

83. *Id.* at 2484.

84. *Id.* at 2485. The government argued that searching cell phone data protects officers by alerting them of confederates in the area, but the Court found this concern was not valid and that this would broaden *Chimel*'s original justification which applied to the ability of the arrestee to use the object as a weapon to resist arrest or escape. *Id.* at 2485–86.

85. *Id.* at 2486. The Court dismissed concerns of remote data wiping, indicating officers could turn off phones or place them in Faraday bags, isolating them from radio waves. *Id.* at 2487.

86. *Id.* at 2487.

87. *Id.* at 2487–88 (comparing this to securing a crime scene while awaiting a warrant).

stake in a cell phone search differ from those in a physical search, implicating *Chimel*'s holding that searching arrestee's home was an impermissible intrusion on the arrestee's privacy.[88] *Riley* determines that arrestees' decreased privacy interest is increased in the context of cell phones compared to searches of physical items.[89] *Riley* therefore limits *Robinson*'s application and adds a layer to the *Robinson* analysis by stating that different considerations must be taken into account as to whether a cell phone found on the arrestee's person may be searched.

Robinson's cigarette packet was not likely to contain any evidence that he was driving without a license, nor was it likely to contain anything with which Robinson might have injured the arresting officer, but *Robinson* holds the search constitutional.[90] Conversely, *Riley* determines that a search of a cell phone which similarly would not have injured the officers nor contain any evidence of the crime for which Riley was arrested was not constitutional. To justify its ruling, the *Riley* Court waxes poetic about the uniqueness of modern cell phones by describing their features and capabilities, comparing them to physical items, and touting their immense storage capacity. The Court describes cell phones as hybrids that contain cameras, calendars, diaries, maps, and newspapers, stating:

> Most people cannot lug around every piece of mail they have received for the past several months, every picture they have taken, or every book or article they have read—nor would they have any reason to attempt to do so. . . .
>
> . . . Cell phones couple that capacity with the ability to store many different types of information: Even the most basic phones that sell for less than $20 might hold photographs, picture messages, text messages, Internet browsing history, a calendar, a thousand-entry phone book, and so on.[91]

The Court also notes four unique features of cell phones that make their unwarranted search more likely to constitute a great intrusion on the privacy of the arrested individual. First, cell phones contain many types of information that reveal more

88. *Id.*

89. *Id.* at 2484–85.

90. United States v. Robinson, 414 U.S. 218, 256 (1973) (Marshall, J., dissenting). *But see Riley*, 134 S. Ct. at 2485 (indicating that the Court has not overlooked this point, but rather than requiring a case-by-case adjudication, asks instead if the application to "this particular category of effects would 'untether the rule from the justifications underlying the *Chimel* exception'" (quoting Arizona v. Gant, 566 U.S. 332, 343 (2009))).

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

in the aggregate than they do individually.[92] Second, the vast capacity of cell phones allows the possessor to store a wealth of data of any individual type.[93] Third, the span of time the data encompasses is far greater than the data an individual would naturally carry on his person.[94] Fourth, the Court notes that most people carry cell phones, and therefore a rule allowing warrantless cell phone searches might have a broader reach than *Robinson* intended.[95]

Riley notes the uniqueness of the type of data cell phones contain, suggesting the *Robinson* Court could never have imagined the type of personal data that can now be recovered from cell phones, indicating that "certain types of data are also qualitatively different."[96] *Riley* explains that web browsing history found on cell phones "could reveal an individual's private interests or concerns—perhaps a search for certain symptoms of disease, coupled with frequent visits to WebMD."[97] The Court also describes concerns regarding location information, suggesting that access to this data would allow police to "reconstruct someone's specific movements down to the minute, not only around town but also within a particular building."[98] The Court goes on to explain that "[t]he average smart phone user has installed 33 app[lication]s, which together can form a revealing montage of the user's life."[99] The Court apparently does not find browsing history or such intensive personal data to be dispositive, however. Companion plaintiff Wurie's cell phone was a

92. *Id.* (noting the possibilities of addresses, notes, prescriptions, bank statements, and videos).

93. *Id.* (explaining the practical difference between a single photo "tucked into a wallet" and "a thousand photographs labeled with dates, locations, and descriptions").

94. *Id.* (comparing a slip of paper in a man's pocket reminding him to call a friend to a record of all communications with that friend over the past several months).

95. *Id.* at 2490 ("Allowing the police to scrutinize such records on a routine basis is quite different from allowing them to search a personal item or two in the occasional case.").

96. *Id.*

97. *Id.*

98. *Id.*

99. *Id.* ("There are apps for Democratic Party news and Republican Party news; apps for alcohol, drug, and gambling addictions; apps for sharing prayer requests; apps for tracking pregnancy symptoms; apps for planning your budget; apps for every conceivable hobby or pastime; apps for improving your romantic life. There are popular apps for buying or selling just about anything, and the records of such transactions may be accessible on the phone indefinitely.").

non-smart phone, a phone type which the Court notes "generally has a smaller range of features than a smart phone" that may not include internet access or a wide array of apps.[100] Nevertheless, the Court holds that the search of such a phone requires a warrant.

The Court also touches on special issues presented by cloud computing, stating that searches of data in the cloud are unconstitutional, but officers—and the owner of the phone—may not know whether a file is stored on the cloud or on the phone, causing further difficulties in searching cell phones.[101]

Riley holds that officers must secure warrants before searching cell phones.[102] It explicitly rejects less practical options, refusing to extend *Gant* to cell phones by restricting access to areas of the phone whose non-digital counterparts were searchable.[103] *Riley* notes how quickly warrants can be obtained[104] and points out that the exigent circumstances exception can be used in instances when the particular situation is so dire as to make a warrantless search reasonable.[105]

D. LOWER COURT INTERPRETATIONS OF *RILEY*

In the months following *Riley*, lower courts have disagreed on the appropriate standard for searches of digital data and how *Riley* should be applied to other smart devices. Interpretations of *Riley*'s application to cell phone searches seem to follow directly from the ruling. For example, one court held that looking at the serial number of the phone is likely a "physical attribute" of the phone itself, not a piece of data, and therefore not considered a search of digital data entitled to *Riley* protections.[106] Another court found that looking at the screen saver of a phone is acceptable under the plain view doctrine.[107]

100. *See id.* at 2481.

101. "Cloud computing is the capacity of Internet-connected devices to display data stored on remote servers rather than on the device itself." *Id.* at 2491.

102. *Id.* at 2485.

103. *Id.* at 2493.

104. *Id.* (citing to the example of a jurisdiction where police officers use iPads to e-mail warrant requests to judges and receive valid warrants in under fifteen minutes).

105. *Id.* at 2494 (listing evidence destruction and pursuit of fleeing suspects as exigencies).

106. United States v. Lowe, No. 2:14-cr-00004-JAD-VCF, 2014 WL 5106053 (D. Nev. Oct. 1, 2014).

107. Sinclair v. State, 118 A.3d 872, 888 (Md. 2015).

However, when applying *Riley* to other smart devices, courts have varied in their interpretations. Some courts hold that *Riley* protects all digital data, on the basis that "*Riley* held unequivocally that digital data is not subject to the warrant exception for searches incident to arrest and . . . officers must obtain a warrant before searching the contents of an arrestee's electronic devices,"[108] and indicate that under *Riley*, citizens now have a "legitimate expectation of privacy in the contents of their electronic devices."[109]

Other courts, however, have eagerly limited *Riley*'s application outside the specific context of cell phones. Courts have found that *Riley* does not prevent searches of credit cards or searches of digital cameras, but even courts agreeing on the result do not agree on the method to determine whether such a search is legal. At least two courts have found that searches of the magnetic stripes on the back of credit and gift cards are not protected under *Riley*.[110] The standards applied by each court to determine the permissibility of these searches were different. One court explained that the "quality and quantity of personal information" on a magnetic stripe was not comparable to that of a smartphone.[111] The other court stated that the amount of data included in the stripe "would not allow officers to reconstruct an individual's private life."[112]

Other courts have addressed the question of *Riley*'s application to digital cameras. Some courts have found that the digital data found on cameras is not protected from a warrantless search incident to arrest.[113] Once again, there appears to be an inconsistency across the courts when it comes to the standard for determining that *Riley* does not protect data on digital cameras. One court found that the camera in question was not protected because it did not have the capabilities of a smartphone, nor were the photos labeled in such a manner that an individual's life could be reconstructed.[114] Another court stated that dig-

108. United States v. Saboonchi, 48 F. Supp. 3d 815, 817 (D. Md. 2015).

109. State v. Purtell, 851 N.W.2d 417, 427 (Wis. 2014).

110. *See* United States v. Bah, 794 F.3d 617, 621 (6th Cir. 2015); United States v. Benjamin, No. 4:14-CR-3089, 2014 WL 5431349, at *4 (D. Neb. Oct. 24, 2014).

111. *See Benjamin*, 2014 WL 5431349, at *3.

112. *See Bah*, 794 F.3d at 633.

113. *See, e.g.*, United States v. Miller, 34 F. Supp. 3d 695, 701 (E.D. Mich. 2014); People v. Raoult, 2d Crim. No. B256148, 2015 WL 3874302, at *1 (Cal. Ct. App. June 23, 2015).

114. *See Raoult*, 2015 WL 3874302, at *3.

ital cameras are not used on a continuous basis like cell phones are, and that "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."[115]

Scholarly commentary indicates that it is not entirely clear how *Riley* should be applied to other devices. The Court's decision to consider *Riley* and *Wurie* together despite the very different phones underlying the two cases may imply that it would be "reasonable for a court to assume that the ability to make and receive phone calls is dispositive, given the Court's grouping together of the general category of cell phones."[116] The Court's joint consideration of *Wurie* and *Riley* might also indicate that any device that implicates more privacy concerns than a non-smart cell phone should not be searched without a warrant.[117] Alternatively, *Riley* might encourage a "contextual approach" in which a court "looks to social norms to determine whether a particular disclosure is 'expected' under the circumstances."[118]

Court readings of *Riley* are clearly inconsistent and will only breed confusion as courts are forced to apply *Riley* to new and varying smart devices. Courts need a singular standard by which to assess the warrant requirements for all smart devices, lest citizens' privacy be better protected when their pictures are on their phones than on their cameras.

E. THE INCREASING UBIQUITY AND CAPACITY OF SMART ACTIVITY TRACKERS

Technology has advanced since *Robinson*'s container search rule, and continues to evolve rapidly.[119] As *Riley* noted, some technological devices are a "pervasive and insistent part of daily life."[120] This is quickly becoming true of smart activity

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

116. Kelly Ozurovich, Comment, Riley v. California—*Cell Phones and Technology in the Twenty-First Century*, 48 LOY. L.A. L. REV. 507, 521 (2014).

117. *Id.*

118. Natasha H. Duarte, *The Home Out of Context: The Post-*Riley *Fourth Amendment and Law Enforcement Collection of Smart Meter Data*, 93 N.C. L. REV. 1140, 1143 (2015).

119. *See* Riley v. California, 134 S. Ct. 2473, 2484 (2014) (noting that ten years previously, smart phones would have been "unheard of," and that even flip phones like Wurie's have existed for less than fifteen years).

120. *Id.* (suggesting cellphones in particular are so commonplace that "the proverbial visitor from Mars might conclude they were an important feature of human anatomy").

trackers, which are worn on the body and allow wearers to toggle through their statistics at the touch of a button.[121] Of all these companies, Fitbit has been particularly successful. It had sold 20.8 million units as of March 2015, and its users include not only your friends and family, but also President Obama and Britney Spears.[122] Additionally, in an analysis of popular mobile applications (apps), Fitbit's app, through which the user can track weight, water, and food intake to supplement the data gathered by the associated device,[123] is the second most popular app associated with a connected device[124] on the Apple and Google Play stores.[125]

The data these devices contain varies by device and, unsurprisingly, the capacity of these devices has become more advanced as time progresses. For illustrative purposes, one can look to the historical development of the devices produced by Fitbit, the most popular smart activity tracker creator.[126] The original Fitbit, often dubbed "Fitbit classic," was first produced

121. *See* Nathan Chandler, *How Fitbit Works*, HOWSTUFFWORKS, http://electronics.howstuffworks.com/gadgets/other-gadgets/fitbit.htm (last visited Mar. 7, 2016) (describing Fitbit's OLED screen, which scrolls through the user's current fitness statistics); Rachael Rettner, *Tracker Craze: Fitness Wristbands' Popularity Will Continue To Grow*, FOX NEWS (Jan. 2, 2014), http://www.foxnews.com/health/2014/01/02/tracker-craze-fitness-wristbands-popularity-will-continue-to-grow ("Fitness trackers . . . are rapidly increasing in popularity, and experts say this trend will continue in the coming years.").

122. *See* Ananya Bhattacharya, *Fitbit Is Now Worth $4.1 Billion After IPO*, CNNMONEY (June 25, 2015, 9:29 AM), http://money.cnn.com/2015/06/17/investing/fitbit-ipo.

123. Though activity tracker devices are frequently linked to apps with which nutritional and weight information are logged, such information is saved on the website itself, not within the wearable device, and is therefore not among the data with which this Note is concerned.

124. Popularity of the Fitbit app is a rough proxy for popularity of the Fitbit devices. Apps connected to outside devices are apps designed (sometimes solely) to gather information from a separate device from the phone itself. The Fitbit app displays the user's daily step tally, calorie burn, active minutes, and sleep quality. This information can only be displayed if the user actually uses a Fitbit device and connects it to the account.

125. *See* Aditi Pai, *Only Google Chromecast's App Is More Popular than Fitbit's in Connected Device Category*, MOBIHEALTHNEWS (Oct. 9, 2014), http://mobihealthnews.com/37214/only-google-chromecasts-app-is-more-popular-than-fitbits-in-connected-device-category (noting that other apps connect to television streaming services, printers, or credit card readers).

126. *See* Robert Hof, *How Fitbit Survived as a Hardware Startup*, FORBES (Feb. 4, 2014, 3:30 PM), http://www.forbes.com/sites/roberthof/2014/02/04/how-fitbit-survived-as-a-hardware-startup (noting that "Fitbit has 77% of the market for full-body activity trackers").

in 2009[127] and tracked steps, distance, activity intensity, and sleep.[128] Fitbit next produced the Fitbit Ultra in 2011, adding an accelerometer that tracked the wearer's elevation, then subsequent models, including the One, Zip, and Flex, which sync wirelessly to cell phones using Bluetooth technology and contain some permutation of the aforementioned features.[129] Newer devices contain heart rate and GPS data.[130] Both existing and potential users have concerns about the privacy implications of tracking this information,[131] and even some elected officials have noted the importance of keeping this "highly personal information" safe.[132]

On the other hand, this data has the potential to be very useful to law enforcement and the judiciary due to its objective and mechanical nature. At least two lawsuits are pending at the time of this writing that rely heavily on Fitbit data. First, in a personal injury suit, data will be used to establish that the plaintiff's quality of life has decreased since an accident due to reduced physical activity.[133] Second, in a criminal prosecution, law enforcement relied on the Fitbit data of a purported rape victim to prosecute her for a false rape report.[134] While the

127. *Id.* (noting that Fitbit classics went up for order in December 2009).

128. *See* Robert J. Nelson, *Everything You Need To Know About Fitbit*, IMORE (June 12, 2014, 8:24 AM), http://www.imore.com/everything-you-need-know-about-fitbit.

129. *See id.*

130. *Charge HR*, *supra* note 11; *Forerunner® 10*, *supra* note 10 (explaining that data can be uploaded "[w]ith a simple connection to your computer").

131. *See* Laura Schooler, *Wearable Technology Future Is Ripe for Growth—Most Notably Among Millennials, Says PwC US*, PRICEWATERHOUSECOOPERS LLP (Oct. 21, 2014), http://www.pwc.com/us/en/press-releases/2014/wearable-technology-future.html (describing a survey in which "82 percent of respondents were worried that wearable technology would invade their privacy and 86 percent expressed concern that wearables would make them more vulnerable to security breaches").

132. *See* Press Release, Charles E. Schumer, Senator, N.Y., Fitbit Bracelets and Smartphone Apps Are Tracking Users' Movements and Health Data that Could Be Sold to Third Parties (Aug. 10, 2014), https://www.schumer.senate.gov/newsroom/press-releases/schumer-reveals-without-their-knowledge-fitbit-bracelets-and-smartphone-apps-are-tracking-users-movements-and-health-data-that-could-be-sold-to-third-parties-calls-for-ftc-to-require-mandatory-opt-out-opportunity-before-any-personal-data-can-be-sold.

133. *See* Moon, *supra* note 17; Nina Zipkin, *Move Over DNA, Your Wearable Data Could Soon Be Used in the Courtroom*, ENTREPRENEUR (Nov. 17, 2014), http://www.entrepreneur.com/article/239869 (hailing this Canadian case as "the first case of its kind" which could set precedent for future claims).

134. *See* Myles Snyder, *Police: Woman's Fitness Watch Disproved Rape Report*, ABC27NEWS (June 19, 2015), http://abc27.com/2015/06/19/police-womans-fitness-watch-disproved-rape-report.

woman had claimed she was sleeping when "an unknown man pulled her out of bed, attacked her in a bathroom, and raped her at knifepoint,"[135] her Fitbit Surge indicated she had been awake and walking around throughout the night.[136] Ultimately, this woman was charged with "false reports to law enforcement, false alarms to public safety, and tampering with evidence" for creating a scene of a struggle.[137] Parties to litigation are already realizing the potential of this data to aid in checking credibility and even to support prosecutions.

It is crucial at this juncture to recognize that smart activity trackers are not the only devices that have the potential to capture more personal data than ever before. Activity trackers are just one manifestation of the recent expansion of the "Internet of Things." This theory describes a not-so-distant future in which "nearly everything that can be connected to the Internet will be."[138] In the "Internet of Things," "[e]verything from televisions to refrigerators to electricity meters will be capable of recording data."[139] Other unique notable examples of the "Internet of Things" include Google Glass,[140] the Apple Watch,[141] and Filip, which is marketed to parents for use by their young children and hosts a limited array of features that nonetheless contain intimate personal information.[142] Developers will inevitably continue to develop advanced technologies for devices that

135. *Id.*

136. *See* Stephanie M. Lee, *As Companies Collect More Health Data, Cops Will Ask To See It*, BUZZFEED (Nov. 5, 2015, 8:00 AM), http://www.buzzfeed.com/stephaniemlee/law-enforcement-requests-for-users-health-and-biometric-data (indicating that the Fitbit model was a Surge).

137. Snyder, *supra* note 134.

138. Brad Turner, *When Big Data Meets Big Brother: Why Courts Should Apply* United States v. Jones *To Protect People's Data*, 16 N.C. J.L. & TECH. 377, 392 (2015).

139. *Id.*

140. *See* Anisha Mehta, Comment, *"Bring Your Own Glass:" The Privacy Implications of Google Glass in the Workplace*, 30 J. MARSHALL J. INFO. TECH. & PRIVACY L. 607, 609 (2014) (describing Google Glass's "ability to continuously record and transmit data within the wearer's surroundings").

141. *See Apple Unveils Apple Watch—Apple's Most Personal Device Ever*, APPLE (Sept. 9, 2014), http://www.apple.com/pr/library/2014/09/09Apple-Unveils-Apple-Watch-Apples-Most-Personal-Device-Ever.html (describing Apple's "most personal device ever," which allows the wearer to transmit their "heartbeat" to another user).

142. *See Stay Connected on Any Adventure: Next Generation Wearable Phone & Locator for Kids*, FILIP, http://www.myfilip.com/about-filip (last visited Mar. 7, 2016) (describing a device that looks like a watch, but contains a GPS tracker and allows the wearer to call five numbers and receive—but not send—text messages).

can be worn on one's person that will contain an increasing quantity of data of an increasingly personal nature. With *Robinson* still guiding the search of physical items, and *Riley* purporting to apply only to cell phones, courts must develop a standard as to how devices between these two extremes should be handled.

II. EXISTING FOURTH AMENDMENT JURISPRUDENCE INDICATES THAT DIGITAL DATA ON ACTIVITY TRACKERS SHOULD BE PROTECTED

The standards lower courts have used when applying *Riley* to magnetic stripes of credit cards and digital cameras indicate a need for a clear and consistent interpretation of *Riley*'s applicability to smart devices that are not cell phones. *Riley* cast additional Fourth Amendment protection over cell phones, holding that an unwarranted search of a cell phone was an unreasonable search. To determine whether an unwarranted search of a smart activity tracker should likewise be considered unreasonable, this Part compares cell phones and activity trackers. It determines that activity trackers contain less data than cell phones, but that the digital data activity trackers hold is extremely personal, and therefore this data merits special treatment from the *Robinson* rule. This Part goes on to discuss the law enforcement need for easily workable and practical rules, the Court's deference to this need, and when the Court has been willing to make exceptions to bright-line rules in the past.

A. CELL PHONES AND ACTIVITY TRACKERS ARE SIMILAR BUT NOT IDENTICAL

Because *Riley*'s outcome is justified by the "pervasiveness of cell phones and their capacity to retain and transport the privacies of life,"[143] it is important to compare the two types of devices. This Section compares cell phones and activity trackers, looking at the way that these devices are carried, their physical capacity to hide weapons, and their societal prevalence. The Section then compares the type and quantity of data that is held by each type of device, as well as methods through which the data is stored.

143. Hillary B. Farber, *Eyes in the Sky & Privacy Concerns on the Ground*, 11 SCITECH LAW., no. 4, 2015, at 6, 9.

1. Comparing the Place of Cell Phones and Activity Trackers in Society and on Our Bodies

Before exploring the data held by each type of device, it is important to compare the physical nature of the devices themselves, as well as their respective places in society. Activity trackers, like cell phones, are frequently carried continuously on one's person, and are therefore likely to be found during a pat down.[144] Activity trackers are perhaps more likely to be found on the person, as they are designed to be worn on the body as an armband or tucked inside of clothing.[145] Activity trackers do not record any personal data if they are not worn on the person.[146] Cell phones, on the other hand, while frequently carried in the pocket, are not always kept there, and may be found just as often in a purse or placed on an adjacent surface.[147] This means that activity trackers are even more likely than cell phones to be found and inspected during searches incident to arrest or during frisks performed under reasonable suspicion.

Activity trackers are fairly similar physically to cell phones both in size and in their lack of capacity to harm officers. Both cell phones and activity trackers tend to fit within the palm of one's hand, though activity trackers are smaller than cell phones.[148] Because the devices are fairly similar physically, they likely hold the same low potential for danger to officers. Despite the relative unlikelihood that a cell phone could conceal a weapon with potential to injure an officer, under *Riley* officers may search cell phones physically to seek out weapons.[149] The

144. *See Worldwide Wearable Computing Market*, *supra* note 15 (referring to fitness trackers as "wearables").

145. *See, e.g.*, *Flex*, *supra* note 2 ("Flex fits comfortably around your wrist . . . so you can wear it day to night."); *One*, *supra* note 3 ("One clips securely and discretely onto your pocket, belt or bra . . . .").

146. *See* Nicole Radziszewski, *Expert Answers: Is It Safe To Wear My Wireless Fitness Tracker All the Time?*, EXPERIENCE LIFE (Nov. 2014), https://experiencelife.com/article/expert-answers-is-it-safe-to-wear-my-wireless-fitness-tracker-all-the-time ("[U]nlike cell phones, activity trackers are meant to be worn on the body around the clock.").

147. Riley v. California, 134 S. Ct. 2473, 2490 (2014) ("According to one poll, nearly three-quarters of smart phone users report being within five feet of their phones most of the time . . . .").

148. *Compare One*, *supra* note 3 (describing the Fitbit One as being 1.89 inches long, 0.76 inches wide, and 0.38 inches thick), *with See all iPhone Models*, APPLE, http://www.apple.com/iphone/compare (last visited Mar. 7, 2016) (listing dimensions of four recent incarnations of the iPhone, which tend to be around five to six inches long and two to three inches wide).

149. *Riley*, 134 S. Ct. at 2485 ("Law enforcement officers remain free to ex-

need to take into account officer safety in light of the potential for concealed weapons should be considered when structuring police rules for handling activity trackers.[150]

Finally, as noted extensively in *Riley*, cell phones are ubiquitous in our society.[151] The Court was quite concerned with the implications of allowing warrantless searches of devices that were so widely carried.[152] At this point, activity trackers are becoming more common but have not reached the societal saturation cell phones have achieved.[153] This might indicate that activity trackers do not need the same protections as cell phones, at least at this time. However, the Court tends to think forward in the context of technology,[154] and with the current level of growth in the activity tracker market,[155] providing greater protections than current numbers might require would be prudent and forward thinking.

2. Activity Trackers Hold Less Data, but More Private Information, than Cell Phones

The crux of whether or not *Riley* should be applied to require warrants to search smart activity trackers is whether the data they contain is similarly private to that of cell phones and thus merits Fourth Amendment protection. This Subsection begins by explaining that while one of the most central features of cell phones is their inherent ability to communicate with ex-

amine the physical aspects of a phone to ensure that it will not be used as a weapon—say, to determine whether there is a razor blade hidden between the phone and its case.").

150. The Court has in the past indicated a willingness to make exceptions to the search incident to arrest exception where there is little to no likelihood of weaponry or evidence of the crime to be found on the arrestee's person. *See* Knowles v. Iowa, 525 U.S. 113, 119 (1998). However, the Court's willingness to allow searches of cell phones for officer safety likely eliminates the possibility of a *Knowles*-style exception here.

151. *Riley*, 134 S. Ct. at 2490 (indicating that "more than 90% of American adults . . . own a cell phone").

152. *Id*. (stating that though police might have "occasionally" stumbled upon a diary in the past, cell phones would crop up far more frequently).

153. *See* Dorene Internicola, *Activity Trackers Get Smarter at Measuring Fitness*, REUTERS (Dec. 22, 2014), http://www.reuters.com/article/2014/12/22/us-fitness-trackers-idUSKBN0K00JJ20141222 (indicating that in the fall of 2013, one in ten American adults wore an activity tracker).

154. *See* Kyllo v. United States, 533 U.S. 27, 37 (2001) ("[T]he technology used in the present case was relatively crude, the rule we adopt must take account of more sophisticated systems that are already in use or in development.").

155. *See* Rettner, *supra* note 121.

ternal devices and individuals, activity trackers generally do not have this ability. On the other hand, the purpose of activity trackers, unlike that of cell phones, is to gather personal data about their user and store it within the device. Finally, this Subsection compares the storage capacity and methods of cell phones and activity trackers and concludes that activity trackers hold far less data then cell phones, albeit data of an inherently private nature.

a. Cell Phones Are Designed for External Communication

In describing the capacity of the modern cell phone, *Riley* focuses most on their capacity to communicate with other devices and individuals.[156] Most modern cell phones have the capacity to connect to the Internet.[157] This ability to connect to the Internet enables and encourages cell phone users to engage in many private and intimate activities, such as banking, Internet browsing, and the downloading and use of apps that yield additional information about the user.[158] The Court's interest in protecting this information from law enforcement seems counterintuitive when considering the fact that in purchasing apps, calling or texting other cell phone users, or engaging in any other Internet-based activity, the cell phone user has necessarily engaged in the sharing of data with third parties, which traditionally has left the user with no reasonable expectation of privacy.[159] This may influence the Court's willingness to reconsider the third-party standard in light of the digital age.[160] However, *Riley* made no explicit statement that users have a reasonable expectation of privacy in any of these types of data. In both *Wurie* and *Riley*, the information gained from the phone had not been shared with anyone—Riley's gang involvement was inferred from photos on his phone, while Wurie's phone yielded a call to a number he labeled as "my house."[161] Some

156. *See Riley*, 134 S. Ct. at *passim* (describing call logs, text messaging, e-mail, voicemail, app downloads, and internet browsing history).

157. *See id.* (describing smartphone capacity to store internet browsing history and connect to the cloud).

158. *See id.* at 2490.

159. *See* California v. Greenwood, 486 U.S. 35, 40 (1988) (holding that because the trash was left on the curb and intended to be handed over to a third party, the owners had no reasonable expectation of privacy in it).

160. *See* United States v. Jones, 132 S. Ct. 945, 957 (2012) (Sotomayor, J., concurring) ("[The third party disclosure] approach is ill suited to the digital age, in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks.").

161. *See Riley*, 134 S. Ct. at 2481.

scholars argue that the third-party exception should be curtailed or limited, as in the modern world "a once small and manageable exception to the Fourth Amendment . . . now threatens to swallow whole the privacy guaranteed by the Fourth Amendment."[162]

Activity trackers, on the other hand, have a more limited ability to connect and share data. These devices can typically only connect to cell phones and computers,[163] which then upload the data to the tracker's associated website or app.[164] Activity trackers are typically not capable of sharing data beyond this limited capacity and cannot communicate from device to device.[165] While there would potentially be a glimmer of an officer safety concern in the context of use of a cell phone to communicate with confederates,[166] no such concern exists with activity trackers.

b. Activity Trackers Gather Different and More Personal Data than Cell Phones

While cell phones are designed to communicate with the outside world, activity trackers are designed to collect data about the way users live their lives, and then display it back to the user.[167] The type of data collected is intimate and private in

162. Turner, *supra* note 138, at 381; *see also* Jane Bambauer, *Other People's Papers*, 94 TEX. L. REV. 205, 262 (2015) (advocating for a restructuring of the third party doctrine).

163. *See, e.g.*, *Flex*, *supra* note 2 (advertising Flex's ability to "sync[] automatically and wirelessly to tablets, computers and . . . smartphones").

164. This connection can be wireless. *See, e.g.*, *id.* (indicating the Flex can "[s]ync stats wirelessly [and] automatically to leading smartphones and computers"); *Up3*, JAWBONE, https://jawbone.com/fitness-tracker/up3 (last visited Mar. 7, 2016) (stating that Up3 "syncs wirelessly using Bluetooth®"). Alternatively, this connection can come through a physical connection. *See Forerunner® 10*, *supra* note 10 (explaining that data can be uploaded "[w]ith a simple connection to your computer").

165. *See, e.g.*, *Fitbit App*, FITBIT, https://fitbit.com/app (last visited Mar. 7, 2016) (indicating that to communicate stats with "friends and followers," a phone or computer is required); *Forerunner® 10*, *supra* note 10 (noting that to communicate with friends, data must be uploaded to a computer).

166. *Riley*, 134 S. Ct. at 2485 (noting that the government entities made an argument that searching cell phones might "alert[] officers that confederates of the arrestee are headed to the scene" and concluding that though this is "undoubtedly a strong government interest," the government entities did not adequately "suggest that their concerns [we]re based on actual experience").

167. *See, e.g.*, *One*, *supra* note 3 (describing the type of data captured and indicating that the device is "discreet"); *Specifications: Display*, FITBIT, https://www.fitbit.com/one#specs (last visited Mar. 7, 2016) (noting that one simply needs to "[p]ush the [display] button to cycle through daily stats" related to

a different way than the data held on a cell phone, as these devices track both personal GPS information[168] and heart rate data.[169] The Court has suggested that GPS data is inherently personal in the context of vehicles,[170] and it is thus likely that courts would find a reasonable expectation of privacy in the non-regulated realm of personal travel.[171] The privacy implications of knowing where an individual goes at which times of the day become even more disturbing when the tracker is located on one's person, indicating travel once an individual exits her vehicle, potentially revealing activity within the home, an area strongly protected under *Kyllo*.[172]

Courts have not yet determined the protective status of heart rate data, but given the Court's past holdings regarding areas protected by the Fourth Amendment, it seems likely that the Court would find this data to be private.[173] Even more so than GPS data, heart rate data has the potential to enable inferences that reveal deeply personal information, such as sleep patterns, sexual activity, physical exertion, and general health,[174] especially when the data is available second by se-

exercise, sleep, and food eaten).

168. *See Forerunner® 10*, *supra* note 10.

169. *See, e.g.*, *Charge HR*, *supra* note 11.

170. United States v. Jones, 132 S. Ct. 945, 956 (2012) (Sotomayor, J., concurring).

171. *See* California v. Carney, 471 U.S. 386, 392 (1985) ("[R]educed expectations of privacy derive . . . from the pervasive regulation of vehicles capable of traveling on the public highways.").

172. *See* Kyllo v. United States, 533 U.S. 27, 34 (2001) ("[O]btaining by sense-enhancing technology any information regarding the interior of the home that could not otherwise have been obtained without physical intrusion into a constitutionally protected area." (internal quotes omitted)).

173. *See, e.g.*, Riley v. California, 134 S. Ct. 2473 (2014) (finding that cell phone searches generally require warrants and cannot be searched under the arrest exception); *Jones*, 132 S. Ct. at 945 (finding the placement of a GPS tracker on a vehicle to be a search); *Kyllo*, 533 U.S. at 27 (finding thermal imaging of the outside of the house to be a search).

174. *See A High Heart Rate—What Can It Possibly Mean for You?*, AZUMIO (Jan. 10, 2013, 12:00 AM), https://www.azumio.com/blog/health/high-heart-rate-and-what-it-means ("A high heart rate can be due to many factors, such as physical activity, panic, stress, or anxiety."); *Is Sex Exercise? And Is It Hard on the Heart?*, HARV. MED. PUBLICATIONS (June 1, 2011), http://www.health.harvard.edu/newsletters_article/is-sex-exercise-and-is-it-hard-on-the-heart (indicating that men's heart rates increase during sexual activity, and that sex ranks as moderate physical activity); *Resting Heart Rate Table*, TOPEND SPORTS, http://www.topendsports.com/testing/heart-rate-resting-chart.htm (last visited Mar. 7, 2016) (displaying resting heart rates with corresponding fitness levels).

cond.[175] This certainly implicates activities within the home, which *Kyllo* protected even when the home is not physically invaded by law enforcement.[176]

Therefore, while cell phones contain bank information, communications with loved ones, and personal pictures,[177] activity trackers contain highly personal heart rate information and GPS data which together have the potential to indicate where users travel and their emotional state while doing so. This is the fundamental purpose of the activity tracker—not simply an incidental function, as GPS data might be considered in the context of cell phones.

c. Activity Trackers Hold Less Data than Cell Phones but the Data Is Intensely Personal

Having looked at the types of data cell phones and activity trackers tend to hold, it is prudent to also compare the storage capacity of the devices. In *Riley*, the Court explicitly noted the great quantity of data that can be held by modern cell phones.[178] Activity trackers hold notably less data than cell phones.[179] Still, these trackers have the capacity to hold several days of very personal data.[180] Additionally, some trackers are designed to automatically delete (or more accurately, record over) data after a certain number of days, whether or not the data has been saved or uploaded to the Internet.[181]

This follows naturally from the different purposes between activity trackers and cell phones. Cell phones function as

175. *See, e.g.*, *Fitbit Help: How Do Fitbit Trackers Sync Their Data?*, FITBIT, http://help.fitbit.com/articles/en_US/Help_article/How-do-Fitbit-trackers-sync-their-data (last visited Mar. 7, 2016).

176. *See Kyllo*, 533 U.S. at 34.

177. *See, e.g.*, *Riley*, 134 S. Ct. at 2489 (discussing cell phone features and storage capacity).

178. *Id.* ("The current top-selling smart phone has a standard capacity of 16 gigabytes (and is available with up to 64 gigabytes). Sixteen gigabytes translates to millions of pages of text, thousands of pictures, or hundreds of videos.").

179. Activity tracker storage information describes storage not in bytes but in days or hours of data, so it is difficult to find a fair way to compare activity trackers and cell phones, but it is likely that fitness trackers hold less data than the average cell phone.

180. *Fitbit Help*, *supra* note 175 ("All Fitbit trackers can record detailed minute-by-minute [calorie burn and sleep] data for seven days . . . [and] heart rate data . . . for 30 days.").

181. *Id.* ("Fitbit Surge can store a maximum of 35 hours of GPS data. If you try to track more than 35 hours worth of GPS data without syncing, older data will be deleted to make room for new data.").

stand-alone devices and therefore have high storage capacities.[182] Activity trackers are designed to sync and upload data to corresponding websites[183] and accordingly need far less storage. Activity trackers also do not present the often-confusing problem of allowing access to files stored on the cloud.[184] The storage capacity of activity trackers is fairly small, but the information that they do hold is vital and personal.

However, the activity tracker context provides another avenue to address the difficult and as-yet unaddressed problem of how data that is uploaded to the Internet should be treated,[185] because activity tracker companies design their devices to nearly require[186] the uploading of data to associated websites. This question is quite interesting in the context of activity trackers because these websites are designed to be tools used by individual users, who have the ability to prevent their information from reaching the eyes of other users.[187] Nonetheless, the fact that the data stored on activity trackers is likely regularly uploaded to the Internet means that under the *Greenwood* third-party standard, there can be no reasonable expectation of privacy in this data.[188]

182. *Riley*, 134 S. Ct. at 2489 ("The term 'cell phone' is itself misleading shorthand; many of these devices are in fact minicomputers that also happen to have the capacity to be used as a telephone. . . . One of the most notable distinguishing features of modern cell phones is their immense storage capacity.").

183. *See supra* note 164 and accompanying text.

184. *Riley*, 134 S. Ct. at 2491 (describing cloud computing as "the capacity of Internet-connected devices to display data stored on remote servers rather than on the device itself," and indicating that this causes trouble for potential searches, as data stored on the cloud may not be searched without a warrant, but the officers may not know if it is stored locally or on the cloud).

185. *See* United States v. Jones, 132 S. Ct. 945, 957 (2012) (Sotomayor, J., concurring) ("[I]t may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties.").

186. It should be noted, of course, that if a wearer is perfectly happy just viewing her daily statistics on the tracker itself each day, many trackers make that a possibility. However, many of the trackers' features are most useful when viewed over several days' time, and most trackers provide only a glimpse at current statistics when users do not upload their data. *See, e.g.*, *App + Dashboard*, FITBIT, https://www.fitbit.com/one#dashboard (last visited Mar. 7, 2016) (showing the Fitbit One screen, which shows a single statistic representative of the day or the moment at which the button is pressed).

187. *One*, *supra* note 3 (displaying data tracked through the Fitbit app on a mobile device or the Fitbit website, which include activity and exercise, weight, food intake, and sleep data).

188. *See* California v. Greenwood, 486 U.S. 35, 40 (1988).

However, the *Riley* Court indicated a healthy respect for the privacy implications digital data can hold, stating that "Internet search and browsing history, for example, can be found on an Internet-enabled phone and could reveal an individual's private interests . . . ."[189] Additionally, Justice Sotomayor suggested in her *Jones* concurrence that the *Greenwood* third-party standard needs to be readdressed because it is "ill suited to the digital age, in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks."[190] These statements were made regarding only the type of digital data collected on GPS devices and cell phones, and the privacy interest would likely be enhanced in the case of activity trackers containing heart rate trackers. This suggests that the intensely personal nature of the data contained on activity trackers might trump its potential to be shared with others.

B. LAW ENFORCEMENT NEED FOR EASILY WORKABLE RULES

The Court has clearly emphasized and prioritized the workability of the rules law enforcement must follow, which often leads the Court to establish clear bright-line rules. *Robinson* describes police decisions as "quick ad hoc judgment[s] which the Fourth Amendment does not require to be broken down in each instance into an analysis of each step in the search"[191] and created a bright-line rule allowing officers to search all arrested persons at the time of arrest.[192] *Riley* more recently noted a preference for police workability, quoting precedent in stating, "[i]f police are to have workable rules, the balancing of the competing interests . . . 'must in large part be done on a categorical basis—not in an ad hoc, case-by-case fashion by individual police officers.'"[193] This practical sentiment led the Court to determine that searching *any* digital data on cell phones—not only data with unsearchable physical counterparts—requires a warrant.[194]

Though bright-line rules may initially appear inflexible, the Court often fashions exceptions where they are necessary.

189. *Riley*, 134 S. Ct. at 2490.

190. *See Jones*, 132 S. Ct. at 957 (Sotomayor, J., concurring).

191. United States v. Robinson, 414 U.S. 218, 235 (1973).

192. *Id.* at 236.

193. *Riley*, 134 S. Ct. at 2491–92 (quoting Michigan v. Summers, 452 U.S. 692, 705 n.19 (1981)) (omission in original).

194. *Id.* at 2495.

Though the Court created *Robinson* as a bright-line rule, it was willing to later make exceptions where the circumstances clearly necessitated different treatment, including an exception based on time passed, an exception for arrestees who receive only citations, and an exception stating that vehicles are to be searched in narrower circumstances than other containers.[195] The Court has also exhibited a particular willingness to allow the exigency exception to supersede bright-line rules. Even when creating *Riley*'s bright-line rule requiring warrants to search all digital data found on cell phones, the Court held that arresting officers may still search digital data where exigent circumstances would otherwise allow them to do so.[196] It appears that the Court prefers to establish clear rules for practical purposes—bright-line rules are easy for officers to follow while in the field, but officers can still employ the exigency exception to warrantless searches in extraordinary circumstances on a case-by-case basis.[197] Law enforcement agencies' need for workable rules to dictate officer conduct in typical situations, as well as superseding exceptions to handle exceptional situations, should guide the solution to the activity tracker problem.

This need is especially applicable in the context of smart wearables like activity trackers—"[i]n the coming world of low-cost wearable technology, requiring police officers to assess every mobile device and render a binary decision as to its capabilities before searching it will not work."[198] After all, ten years ago no one knew that pedometers would be capable of storing days' worth of GPS and heart rate data. Today that is the norm. In the future, when the "Internet of Things" becomes a reality, courts and law enforcement agencies will absolutely require a simple bright-line rule that can be applied broadly to all developing wearable technologies.

195. *See supra* Part I.B.1.

196. *Riley*, 134 S. Ct. at 2494.

197. *Id.* ("The critical point is that, unlike the search incident to arrest exception, the exigent circumstances exception requires a court to examine whether an emergency justified a warrantless search in each particular case.").

198. Patrick Brown, Note, *Searches of Cell Phones Incident to Arrest: Overview of the Law as It Stands and a New Path Forward*, 27 HARV. J.L. & TECH. 563, 575 (2014).

III. WHEN SEARCHING ARRESTEES' EFFECTS INCIDENT TO ARREST, LAW ENFORCEMENT OFFICERS SHOULD DIFFERENTIATE BETWEEN PHYSICAL OBJECTS AND DIGITAL DATA

Riley essentially recognized the innate differences between physical objects, such as the cigarette package searched in *Robinson*, and digital containers like cell phones, which hold far more than *Robinson* would have anticipated.[199] Courts should extend the cell phone exception to cover the digital data found in activity trackers and similar devices because the government's interest in the search incident to arrest exception does not adequately outweigh the great degree of intrusion upon the defendant's privacy in the intensely private activity tracker data.[200]

The ideal solution is for courts and law enforcement officers to adopt a two-tiered approach that considers separately the authority of officers to search the physical object and the digital data it contains. Under such an approach, the physical aspects of any digital container may be searched warrantlessly when it is found incident to a lawful arrest, but to access the digital data these containers hold, officers would need to secure a warrant. This solution is strongly supported by both case law and policy concerns. By recognizing the distinction between physical and digital evidence as *Riley*'s essential holding, courts can ensure that all digital data is protected adequately and immediately. Until courts explicitly hold that *Riley* applies evenly to all smart devices, an argument can still be made that *Riley* applies solely to cell phones, and courts will be forced to analyze each device and its similarities and dissimilarities to cell phones. As demonstrated by various courts' application of *Riley* to digital cameras and credit cards, this type of individual analysis breeds inconsistency and is a waste of judicial resources.

This Part describes that under this two-tiered framework, arresting officers have the capacity to physically examine the external case and body of the activity tracker without first obtaining a warrant. This Part goes on to explain that conversely,

199. *Riley*, 134 S. Ct. at 2485 ("A search of the information on a cell phone bears little resemblance to the type of brief physical search considered in *Robinson*.").

200. *See* Wyoming v. Houghton, 526 U.S. 295, 300 (1999) (indicating that searches must be assessed by balancing legitimate government interests against the degree of intrusion upon an individual's privacy).

officers must obtain warrants to search digital data on activity trackers. This Part will then explain that the exigency exception will continue to allow officers to search through the data when they believe that the data will be deleted otherwise. Finally, this Part will caution that adequate training of law enforcement officers is crucial for the protection of arrestees' private data.

A. PHYSICAL EXAMINATIONS OF ACTIVITY TRACKERS MAY BE PERFORMED WARRANTLESSLY

Though there is no danger of injury from the digital data contained within these devices, law enforcement officers should be able to physically examine these devices. These physical searches should be brief inspections of the physical device itself, for the purpose of ensuring that it is not a weapon[201] and does not contain any weapons within it or its accompanying case, such as pins or razor blades.[202]

Problematically, in such a physical inspection, law enforcement officers might not recognize activity trackers because these devices are not yet nearly as prevalent as cell phones in our society[203] and they may not all be easily recognizable as being activity trackers.[204] This means an officer might access digital information by clicking the button on the device and viewing the user's daily statistics, possibly without even realizing what data she is accessing. While clicking the button of an unknown device to ensure its functionality and that it is not merely a shell concealing a weapon might be considered acceptable, toggling through daily statistics would constitute a search requiring a warrant in much the same way that searching

201. One could see, for example, why a shoe-based tracker like the SmartMove shoe insole, *see* Truong, *supra* note 4, could arouse suspicions in light of at least one attempted shoe bombing. *See Shoe Bomber: Tale of Another Failed Terrorist Attack*, CNN (Dec. 25, 2009, 10:23 PM EST), http://www.cnn.com/2009/CRIME/12/25/richard.reid.shoe.bomber.

202. *Riley*, 134 S. Ct. at 2485 (allowing officers, for example, to "determine whether there is a razor blade hidden between the phone and its case"); United States v. Robinson, 414 U.S. 218, 257 (1973) (Marshall, J., dissenting) (suggesting that even when finding envelopes, the *Robinson* standard would allow a search for safety purposes in case pins or razor blades were hidden within).

203. *See supra* Part II.A.1. *But see* Rettner, *supra* note 121 (indicating the rapid growth of the activity tracker market).

204. *See, e.g.*, *Flex*, *supra* note 2 (wristband); *One*, *supra* note 3 (clip-on device); Truong, *supra* note 4 (shoe insole).

through text messages or photos on a cell phone would require a warrant.[205]

Law enforcement agencies should seek to avoid unconstitutional searches, and brief training on the available types of wearable technology might go a long way towards this goal. In the wake of *Riley*, law enforcement agencies should thoroughly train their officers as to existing wearables, including smart activity trackers, and the data these devices are capable of holding. Such training need not be lengthy, and could be done in the form of a handout or an email, provided officers were required to read it. However, such training should be updated fairly frequently for two reasons. First, it will increase officer understanding of what they may lawfully search at the time of arrest, and as a result will protect the civil liberties of those searched incident to arrest. Second, this training, if kept up-to-date, will ensure that arresting officers realize the potential treasure troves of relevant evidence at their fingertips and apply for warrants in a timely manner to ensure that data is gathered.

B. TO SEARCH DIGITAL DATA, OFFICERS MUST OBTAIN WARRANTS ABSENT EXIGENT CIRCUMSTANCES

Digital data on activity trackers should be protected as much as possible from warrantless searches because it is deeply personal information. This Section explains that generally officers should not be allowed to search this digital data without acquiring a warrant. However, this Section will go on to explain that the exigent circumstances exception might be used more often for activity trackers than for cell phones and will provide officers with the necessary discretion to warrantlessly search in emergency situations.

1. Officers Generally May Not Search Digital Data Without a Warrant

Some activity trackers contain incredibly personal data, including heart rate and GPS data.[206] While some smart activity trackers hold less important data than others,[207] each new device collects more advanced types of data.[208] Additionally, the

205. *See infra* Part III.B.1.

206. *See, e.g.*, *Charge HR*, *supra* note 11 (heart rate); *Forerunner® 10*, *supra* note 10 (GPS).

207. *See, e.g.*, *Zip*, *supra* note 3 (tracking only steps, calorie burn, distance traveled, and relative activity).

208. *See supra* Part I.E (describing the historical development of Fitbit, the

discrepancy between high-tech and low-tech activity trackers is comparable to that seen in Riley's smart phone and Wurie's flip phone.[209] The Court created a bright-line rule for all cell phones, not just smart phones. For the same reasons, courts and law enforcement officers should protect all activity trackers by requiring a warrant to access any digital data on an activity tracker. Either connecting the tracker to a computer or manually toggling through this data on the tracker itself would constitute a search and would require a warrant.[210]

One could argue that only the more personal forms of data should be protected, allowing officers to access step count or flights of stairs climbed without a warrant. However, this is impractical for two reasons. First, this would require officers to determine, at the time of arrest, which pieces of information are private and are not. This is a difficult determination to make in a split second, and would not produce a workable rule.[211] Second, the physical nature of activity trackers would make such a rule even less workable. These trackers tend to have a single button allowing the data to come across the screen one by one,[212] or do not have screens and require an upload to a computer, which instantly uploads all information from the tracker, unlimited by time or type.[213]

An argument that law enforcement officers should be allowed to warrantlessly search digital data if they would be able to search the physical counterpart[214] was also rejected in *Riley*. Not only does this fail to provide a workable rule for law enforcement,[215] but also many of the types of data collected and

leading producer of activity trackers).

209. *See* Riley v. California, 134 S. Ct. 2473, 2480–81 (2014) (describing Riley's smart phone as having "a broad range of other functions" and Wurie's flip phone as having "a smaller range of features").

210. *Cf. id.* at 2492–93 (finding that looking through data on the phone itself was an unreasonable search where no warrant was obtained beforehand).

211. *See id.* at 2491 (stating the Court's "general preference to provide clear guidance to law enforcement through categorical rules"); United States v. Robinson, 414 U.S. 218, 235 (1973) (indicating these decisions are "quick ad hoc judgment[s]").

212. *See Charge HR*, *supra* note 11; *One*, *supra* note 3; *Specifications: Display*, *supra* note 167; *Zip*, *supra* note 3; *supra* note 167 and accompanying text.

213. *See, e.g.*, *Flex*, *supra* note 2; *Up*, *supra* note 2.

214. *See, e.g.*, *Riley*, 134 S. Ct. at 2493 (discussing this argument in the context of cell phones).

215. *Id.* (objecting to the bulk of data that could be recovered and stating such a test would require "a difficult line-drawing expedition to determine which digital files are comparable to physical records," leaving it "[un]clear

stored on activity trackers have no non-digital counterpart. Courts would be forced to first determine non-digital counterparts for each type of data—for instance, is a map a non-digital counterpart of GPS data, or must it be manually labeled with timestamps?—and second, determine whether the substitute would be protected. Such a process would take far too long to be a workable rule for law enforcement officers.

Finally, it should be noted that the process of actually obtaining warrants need not be seen as a barrier—in fact, the efficiency of this process in the modern world was noted in *Riley*.[216] Warrants for these devices would, of course, face some challenges,[217] but this is true of all warrants for digital data, including the cell phone warrants prescribed by *Riley*. The fact that the warrant application process is in flux should be no barrier to this workable and practical solution.

2. The Exigency Exception Would Enable Officers To Search Digital Data on Activity Trackers in Emergency Circumstances

Despite the speed at which warrants can be obtained,[218] the Court found in *Riley* that across-the-board rules without explicit exceptions do not adequately protect officer safety, and therefore found that officers were entitled to search digital data on cell phones in exigent circumstances.[219] Due to the fairly similar nature of activity trackers to cell phones, officers should be able

how officers could make these kinds of decisions before conducting a search, or how courts would apply the proposed rule").

216. *Id.* (indicating that in some jurisdictions warrants can be requested via iPad and can be signed and returned to the officer on the scene within fifteen minutes of the request).

217. *See, e.g.*, James Saylor, Note, *Computers As Castles: Preventing the Plain View Doctrine from Becoming a Vehicle for Overbroad Digital Searches*, 79 FORDHAM L. REV. 2809, 2847 (2011) (describing the conflict of reconciling the plain view exception, allowing officers to use anything in plain view, with modern searches of digital data where all data is downloaded at once). For a discussion of what such warrants should look like, see generally Andrew D. Huynh, Note, *What Comes After "Get a Warrant": Balancing Particularity and Practicality in Mobile Device Search Warrants Post-*Riley, 101 CORNELL L. REV. 187 (2015), and Paul M. Ervasti, *Is the Particularity Requirement of the Fourth Amendment Particular Enough for Digital Evidence?*, ARMY LAW., Oct. 2015, at 3, 3.

218. *Riley*, 134 S. Ct. at 2493.

219. *Id.* at 2486 ("[T]he interest in protecting officer safety does not justify dispensing with the warrant requirement across the board. To the extent dangers to arresting officers may be implicated in a particular way in a particular case, they are better addressed through consideration of case-specific exceptions to the warrant requirement, such as the one for exigent circumstances.").

to rely on the exigency exception to search digital data on the scene under exceptional circumstances.

For illustrative purposes, imagine that officers have been investigating a cocaine smuggling ring and have pinpointed one suspect whom they believe to be involved. Officers believe, from the patterns of cocaine availability in the community, that the suspect meets with the kingpin of the ring on Sundays at a consistent time and location. The officers believe if they can determine the location of these meetings, they will be able to use that information to identify other members of the ring. Suppose the suspect is arrested on a Monday afternoon wearing an activity tracker with GPS data that is automatically deleted every twenty-four hours. In that instance, arresting officers might not be able to afford waiting to obtain a warrant—the suspect likely visited the location in question within 24 hours and the relevant data has the potential to be deleted within minutes. Those officers, under the two-tiered approach, would be allowed under the exigency exception to download the data before it was deleted in order to find the location of the meeting place of the drug smugglers. Thus, when there is probable cause to believe that evidence on the tracker will be destroyed or deleted, as in the case of heart rate data that will be deleted in seven days,[220] officers should be allowed to access the data before a warrant can be obtained and before the data will be lost.

It is important to note that without officer training, the good faith exception could swallow the rule by allowing activity tracker data gathered during improperly warrantless searches to be presented at trial where the law enforcement officer believed in good faith that he could search the device.[221] An officer who knows only that wearables contain helpful information and that some of them delete their data on a periodic basis might mistakenly search all wearables for fear of destruction of evidence. For this reason, training is all the more important. It may be wise for courts to bar introduction of evidence where such evidence is admissible only under the good faith exception and the officer had not been properly trained regarding smart wearables. This would strongly encourage law enforcement agencies to ensure that their officers were properly trained.

220. *See Fitbit Help*, *supra* note 175 (indicating that some data is deleted as soon as thirty-five hours after it is collected, while some remains on the device for several weeks).

221. *See generally* United States v. Leon, 468 U.S. 897 (1984) (considering the implications of officer training with regards to the good faith exception).

The exigency exception will therefore prevent the two-tiered approach from tying the hands of law enforcement in circumstances in which officers have no choice but to either access the data or see it lost forever.[222]

C. COUNTERARGUMENTS TO THE TWO-TIERED SOLUTION CANNOT PREVAIL

Several potential counterarguments to this Note's proposal to protect activity tracker data can be predicted. Still, no counterargument unseats the two-tiered approach as the most logical way to approach searches of activity tracker data.

First, some might suggest that data of activity trackers is not accurate enough to warrant protection.[223] There have not yet been any court determinations of the accuracy of activity tracker evidence, or how strongly such data may be relied upon. Heart rate data in particular can be critiqued on the following basis: even if a heart rate is high, it is not clear why it is elevated.[224] Such a reliability determination is outside the scope of this Note. It should be noted, however, that in a civil suit in Canada, Fitbit data has been used to support a personal injury claim.[225] Moreover, law enforcement has relied on Fitbit data in at least one prosecution,[226] and the government has requested activity tracker data from at least one activity tracker producer, indicating that law enforcement officers think this information is valuable in some contexts, whether or not it will be admissible in court.[227] Additionally, it is important that courts

222. Additionally, it may be possible in such circumstances for law enforcement officers to subpoena the related companies for the desired information. *See* Gabriel R. Schlabach, Note, *Privacy in the Cloud: The Mosaic Theory and the Stored Communications Act*, 67 STAN. L. REV. 677, 679–80 (2015) (indicating that even where law enforcement officers can and do acquire information through this process, the result is a "mosaic" of the data).

223. *See* Elizabeth Murray, *Fitbit Lawsuit Alleges Heart Rate Monitors Are Inaccurate, Misleading*, TODAY (Jan. 8, 2016, 7:40 AM), http://www.today.com/health/fitbit-lawsuit-alleges-heart-rate-monitors-are-inaccurate-misleading-t65956 (describing a recent lawsuit brought by Fitbit customers against the company, claiming that its heart rate trackers do not always properly display accurate heart rates).

224. *See* sources cited *supra* note 173 (suggesting the Supreme Court would likely find heart rate data private).

225. *See* Alexander Howard, *How Data from Wearable Tech Can Be Used Against You in a Court of Law*, HUFFINGTON POST (June 30, 2015, 2:41 PM), http://www.huffingtonpost.com/alexander-howard/how-data-from-wearable-te_b_7698764.html.

226. *See* Schooler, *supra* note 131.

227. *See* Lee, *supra* note 136 (indicating that Fitbit has received requests

not allow any perceived inaccuracy of modern day activity trackers to prevent law enforcement officers from using data from future, more advanced, and technically accurate devices.

Second, critics might argue that activity trackers do not hold enough data to earn the same protection as cell phones. No matter the quantity of data on activity tracker, it is so comprehensive that it must be protected.[228] *Riley* emphasized that cell phone data "form[s] a revealing montage of the user's life."[229] The GPS, heart rate, calorie burn, flights of stairs, and other data found on activity trackers similarly would allow law enforcement officers to reassemble the user's life. This data should therefore be protected.

Finally, critics might suggest that protection is not needed because some activity trackers automatically delete their data after a certain amount of days. It is crucial to note, however, that in the modern world, a warrant can be obtained in as little as fifteen minutes.[230] Arguments that activity trackers' automatic deletion of data should entitle the officer to a warrantless search are therefore unlikely to be persuasive in most circumstances.[231]

A two-tiered approach with separate requirements for searching the physical object and the digital data it contains is the ideal flexible solution to cover all wearables, including smart activity trackers. Employing such a standard would require officer training to recognize wearables and search their exteriors for concealed weapons while refraining from searching their digital contents. This training would also teach officers about the types of data that can be held by various wearables and the importance of obtaining a timely search warrant to access this potentially invaluable data. This solution therefore

from law enforcement agencies for data of individual customers).

228. *See* Andrew Pincus, *Evolving Technology and the Fourth Amendment: The Implications of* Riley v. California, 2014 CATO SUP. CT. REV. 307, 329 n.86 (noting that some "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" causes it to fit under the *Riley* umbrella).

229. Riley v. California, 134 S. Ct. 2473, 2490 (2014).

230. *See id.* at 2493.

231. It is also crucial to note that with the training this Note recommends, officers should be more likely to know which trackers delete their data within hours rather than weeks. Additionally, they would be more likely to know whether a particular activity tracker will soon delete the relevant data, and thus know whether exigent circumstances truly exist.

maximizes individual privacy rights, officer safety, and law enforcement productivity.

CONCLUSION

In *Riley*, the Court held that cell phones were meaningfully different from non-digital objects found on arrestees in searches incident to arrests due to the type and quality of data they are capable of holding. In holding that searching cell phones found incident to arrest requires a warrant, the Court indicated that digital data was qualitatively different from physical objects found during pat downs. After the Court decided *Riley*, smart activity trackers have continued to gain popularity and their features continue to advance. Now that *Riley* has suggested at least some digital data is given more zealous protection than physical objects, law enforcement officers need a standard for how and when smart activity trackers and other wearables may be searched at the scene of arrest and when a warrant is required.

The best way to resolve this problem is to create a two-tiered approach distinguishing between searches of physical objects and the digital data they contain. Such an approach would allow officers to inspect the physical activity trackers for potential danger, but not to look through or search digital data before obtaining a warrant to do so. In a circumstance in which the officer believes that exigent circumstances exist in the form of inevitable deletion of evidence relevant to the crime of arrest, the officer is free to access the data and the courts can later address her actions. Finally, government entities and officers must be made aware of the wide array of smart devices that exist, including smart activity trackers. Awareness and understanding of these devices will be key to appropriately balancing government interests and citizen privacy.