COMMENT

A CASTLE IN THE SKY: GPS TRACKING OF A DEFENDANT'S CELL PHONE POST–*RILEY V. CALIFORNIA*

BRYAN SANDFORD*

For most Americans, "smart" cell phones are an omnipresent fact of life. The technological capabilities of these devices have had a transformative effect on the way we do business, communicate, and socialize with one another. One capability in particular, the ability to track and broadcast a user's location in real time, presents a danger in the context of the Fourth Amendment: that privacy in one's location will become a relic of the past. Though the judiciary's role as to this issue is still being fleshed out, courts should hesitate before discarding privacy in favor of law enforcement efficiency and carefully scrutinize searches that tip the scales too far in either direction. Thus far, however, courts are struggling with how to address law enforcement efforts to access cellular location and real-time GPS information. Though the Supreme Court has provided some guidance, it appears reluctant to clarify the role that the Fourth Amendment plays in limiting access to GPS data.

In its latest decision on the Fourth Amendment and new technology, a unanimous Court discussed the enormous privacy implications attendant to unrestricted law enforcement access to the digital contents of one's cell phone. This Comment discusses the implications that *Riley v. California* has on the Fourth Amendment analysis of GPS tracking by law enforcement. It argues that the Court implicitly created a *per se* rule requiring a warrant before accessing any content within a cell phone—which necessarily includes GPS data. The Court's methodology in recent decisions and comparison to other contexts where the Court has created *per se* warrant requirements support this conclusion. In light of this, this Comment posits that lower courts should determine on a case-by-case basis whether the policy and reasoning of *Riley* support applying various warrant exceptions to GPS tracking. It discusses which warrant exceptions should apply, using four lower court approaches—from Wisconsin, Florida, and the Fifth and Sixth Circuits—as templates. Finally, it suggests that the Court should revisit and clarify this issue, which will aid state legislatures and lower courts in their efforts to determine the constitutional requirements.

---

* J.D. Candidate, May 2016, University of Wisconsin Law School. I want to thank Professor Byron Lichstein for alluding to this topic by discussing this issue and his work with *Subdiaz-Osorio*. I also want to thank Professor Keith Findley and Laura Bachmann for their support; this article would have been impossible without it. Finally, thanks to Professor Anuj Desai, Nick Yurk, Cameron Marston, and the others at the *Wisconsin Law Review* for their feedback and hard work.

INTRODUCTION

To say that cell phones have become omnipresent in the United States would not overstate the significant impact these devices have had on our society. Numerous works on this topic have charted the explosive growth of both cellular technology in general and the smart phone.[1]

1. *Compare* Kevin McLaughlin, Note, *The Fourth Amendment and Cell Phone Location Tracking: Where Are We?*, 29 HASTINGS COMM. & ENT. L.J. 421, 421–22 (2007) (explaining that there were 195 million cell phone subscribers in the

Given the ever-accelerating pace of new technology and attendant law enforcement applications, it is not surprising that courts have struggled to keep up. Indeed, one wonders whether the Supreme Court's caution in new technological areas is still appropriate,[2] given the speed with which new innovations are ubiquitously adopted and the corresponding encroachment into traditionally private areas and activities.[3]

This Comment considers whether the Court's latest decision on the intersection between the Constitution and technology applies to the tracking of a criminal suspect's cell phone by its Global Positioning System (GPS). The Court in *Riley v. California*[4] held that, at least within the scope of the search-incident-to-arrest doctrine, police must generally have a warrant to search data on a cell phone.[5] What is less clear from that opinion is how broadly the rule applies.[6] Does *Riley*

U.S. in 2007, which was twice as many as in 2003), *with CTIA's Wireless Industry Indices: 1985 – 2005*, CTIA, http://www.ctia.org/your-wireless-life/how-wireless-works/annual-wireless-industry-survey (last visited Oct. 12, 2015) (over 355 million as of Dec. 2014, which represents an annual increase of 20 million compared to 2013).

2. *See City of Ontario v. Quon*, 560 U.S. 746, 759 (2010) ("The judiciary risks error by elaborating too fully on the Fourth Amendment implications of emerging technology before its role in society has become clear." (citation omitted)). For a discussion of how *Riley* may signal a change in the attitudes of the Court regarding its role with respect to new technologies, see Andrew Pincus, *Evolving Technology and the Fourth Amendment: The Implications of* Riley v. California, 2013–2014 CATO SUP. CT. REV. 307, 307–08, 329–36 (2014).

3. *See generally* Muhammad Usman Iqbal & Samsung Lim, *Privacy Implications of Automated GPS Tracking and Profiling*, IEEE TECH. & SOC'Y MAG., Summer 2010, at 39, 39–41, 46. It is somewhat ironic that the Fourth Amendment jurisprudence of previous eras so often centered around phone booths. *See, e.g.*, *Katz v. United States*, 389 U.S. 347, 348–50 (1967). The phone and privacy interests may have changed, but balancing those interests against law enforcement need remains the same.

4. 134 S. Ct. 2473 (2014).

5. *Id.* at 2485 ("We therefore decline to extend [the search incident to arrest exception] to searches of *data on cell phone*s, and hold instead that officers must generally secure a warrant before conducting a search." (emphasis added)).

6. *See* Michael D. Ricciuti & Kathleen D. Parker, *My Phone is My Castle: Supreme Court Decides that Cell Phones Seized Incident to Arrest Cannot Be Subject to Routine Warrantless Searches*, 58 BOS. B.J., Fall 2014, at 7, 9. In an early article discussing *Riley*, Ricciuti & Parker state:

> It remains to be seen how *Riley* will apply to future cases where the government seizes information closely related to cell phone use, such as cell-tower tracking data, which can pinpoint a user's location even in real time . . . . But *Riley* and the cases that preceded it make clear that the Court is adapting to the times and will not blindly apply law from an earlier age to today's digital media.

Id. Other commentary has concluded that "the Fourth Amendment is likely not implicated by *historical* cellular location information," and instead proposes legislative and law enforcement solutions. Nathaniel Wackman, Note, *Historical Cellular Location Information and the Fourth Amendment*, 2015 U. ILL. L. REV. 263, 263 (emphasis

merely create a *per se* exception to an exception,[7] or does the decision create a bright-line warrant requirement applicable to all contexts in which law enforcement might access a phone?[8] This Comment argues that a broad reading of *Riley* is the logical extension of the Court's Fourth Amendment jurisprudence.

The latter reading of *Riley* has significant implications for GPS tracking of a suspect's cell phone—an increasingly common practice among law enforcement.[9] Prior to *Riley*, the Court's only guidance for analyzing GPS searches came from dicta in *United States v. Jones*.[10] In *Jones*, Justice Scalia's majority opinion stated that the proper standard to analyze GPS tracking when no physical trespass occurs is the reasonable expectation of privacy test.[11] Recent decisions, including a high profile GPS phone tracking case from the Wisconsin Supreme Court, have followed these dicta in *Jones*,[12] while others have viewed *Riley* as signaling a change in attitude regarding searches of cellular data.[13]

---

added). This Comment focuses on real-time GPS tracking, which involves significantly more "contact" with information stored within the phone itself. *See infra* Part II.C.3.

7. That is, by creating an exception to the search-incident-to-arrest warrant exception.

8. *See* Adam Lamparello & Charles E. MacLean, Riley v. California*: Privacy Still Matters, but How Much and in What Contexts?*, 27 REGENT U. L. REV. 25, 33 (2014) (concluding that *Riley* created a categorical bright-line rule premised in reasonableness unlike many prior "ad-hoc" decisions that applied *Katz*); *cf., e.g.*, *Payton v. New York*, 445 U.S. 573, 589–90 (1979) (creating such a bright-line requirement for entries into the home). The Court in *Payton* stated "the Fourth Amendment has drawn a firm line at the entrance to the house. Absent exigent circumstances, that threshold may not reasonably be crossed without a warrant." *Id.* at 590. *Payton*'s language is strikingly similar to that used in *Riley*. *Riley*, 134 S. Ct. at 2482 ("In the absence of a warrant, a search is reasonable only if it falls within a specific exception to the warrant requirement."); *see infra* Part II.C.1.

9. *See, e.g.*, *State v. Subdiaz-Osorio*, 824 N.W.2d 748, 755, 757 (Wis. 2014); *see also* John S. Ganz, Comment, *It's Already Public: Why Federal Officers Should Not Need Warrants to Use GPS Vehicle Tracking Devices*, 95 J. CRIM. L. & CRIMINOLOGY 1325, 1325–27 (2005); Iqbal & Lim, *supra* note 3, at 46.

10. 132 S. Ct. 945, 953 (2012).

11. *Id.* at 953; *see also Katz v. United States*, 389 U.S. 347, 361 (1967) (Harlan, J., concurring).

12. *Subdiaz-Osorio*, 824 N.W.2d at 764. Lower federal decisions split into *primarily* two categories pre-*Riley*, at least with respect to historic cell site location information. *See* Wackman, *supra* note 6, at 293 (describing three categories). One of the categories treats cell site location information like tracking cases and often follows the dicta in *Jones*. *See id.* at 301–08.

13. *Compare Subdiaz-Osorio*, 824 N.W.2d at 763–64 *and Tracey v. State*, 152 So. 3d 504, 514–15 (Fl. 2014) (viewing *Katz* as the controlling standard), *with United States v. Stile*, 1:11-cr-00185-JAW, 2014 U.S. Dist. LEXIS 144241, at *10 (D. Me. Oct. 10, 2014) (assuming that *Riley* would apply beyond search-incident-to-arrest).

Under the proposed reading of *Riley*, the propriety of warrantlessly accessing cellular GPS data would turn on whether such access fit within an exigent circumstance or other warrant exception, rather than focusing on the threshold search question.[14] Such a bright-line warrant requirement follows the underlying reasoning of *Riley* and creates consistent results in an area the Court is treating with increasingly greater Fourth Amendment protection. In light of this, *Riley* should be interpreted as standing for the following: first, that individuals and society have a reasonable expectation of privacy in their cell phone's GPS data; second, that a search necessarily occurs when GPS data is accessed; and finally, that such a search is unreasonable in the absence of a warrant or exception.[15]

While other works have discussed what application *Riley* could have beyond search incident to arrest,[16] most focus on the effect the decision will have on the collection of metadata and historical cell site information.[17] By contrast, this Comment focuses primarily on GPS tracking conducted in real time, as such tracking involves a direct access to the data contained within a phone.[18] It argues that the language and reasoning of *Riley* extend to this type of direct intrusion.

---

14. *See infra* note 38. The judicial evaluation as to the expectation of privacy one has in not being tracked by GPS is, at best, a legal fiction. *See Subdiaz-Osorio*, 824 N.W.2d at 760, 766–68 (discussing the difficulties of applying the *Katz* test to GPS cell phone tracking and deciding instead to assume an expectation of privacy without deciding); 1 WAYNE R. LAFAVE, SEARCH AND SEIZURE: A TREATISE ON THE FOURTH AMENDMENT § 2.1(d) (3d ed. 1996); Richard A. Posner, *The Uncertain Protection of Privacy by the Supreme Court*, 1979 SUP. CT. REV. 173, 188 (discussing the "circular" nature of the *Katz* inquiry).

15. *See, e.g.*, *Tracey*, 152 So. 3d at 524–26. A way to conceptualize this view of *Riley* is that the test in *Katz* is *per se* satisfied whenever the data on a cell phone is accessed by law enforcement. *See* Lamparello & MacLean, *supra* note 8, at 38–39; *see also* Orin S. Kerr, *The Mosaic Theory of the Fourth Amendment,* 111 MICH. L. REV. 311, 312–14 (2012); Wackman, *supra* note 6, at 307–10. And if a search occurs every time a cell phone's GPS data is accessed by law enforcement, then in the absence of a warrant, such a search would be unreasonable unless an exigent circumstance or other *permissible* warrant exception is present. *See Riley v. California*, 134 S. Ct. 2473, 2482, 2494 (2014).

16. *See, e.g.*, Lamparello & MacLean, *supra* note 8, at 33–41; *see also* Peter Margulies, *Dynamic Surveillance: Evolving Procedures in Metadata and Foreign Content Collection After Snowden*, 66 HASTINGS L.J. 1, 42–43 (2014); Ricciuti & Parker, *supra* note 6, at 9.

17. *See, e.g.*, Margulies, *supra* note 16, at 43; Wackman, *supra* note 6, at 293.

18. To frame the discussion that follows several issues should be understood. First, this Comment uses the term "real-time GPS tracking" which is actually a misnomer: such tracking encompasses all real-time tracking of a cell phone, which is usually based on a combination of data including GPS, cellular, wireless (WiFi) networks, etc. *See infra* Part I.A. Second, real-time GPS tracking is distinct from historical tracking in that the former involves active requests from law enforcement to a

Part I of this Comment briefly examines the technology GPS tracking and the Fourth Amendment jurisprudence that governs searches of a defendant's property and location. Part II discusses GPS tracking by law enforcement, analyzes how *Jones* and *Riley* apply to such tracking, and contends that the Court has implicitly created a new standard for GPS tracking of cell phones. Namely, *Riley* implies that accessing cellular data in real time always constitutes a search under *Katz* and therefore the inquiry shifts to whether the search was executed pursuant to a warrant or permissible exception.[19]

Part III examines different judicial approaches taken after *Riley* to the issue of whether a warrant is required to track a cell phone.[20] It also

---

cellular provider who in turn obtains location information transmitted from the phone. *See infra* Part I.A. To over-simplify, for most smart phones it is impossible for the phone to broadcast its location without analyzing information received from the providers' remote server (which "assists" the smart phone by handling most of the heavy lifting involved in translating GPS satellite signals to triangulate position). *See infra* text accompanying notes 28–30. Third, it is also important to note that prior to *Riley*, courts were more willing to overturn cases involving tracking in real time, likely because the third-party doctrine is less implicated. *See* R. Craig Curtis, Michael C. Gizzi & Michael J. Kittleson, *Using Technology the Founders Never Dreamed of: Cell Phones as Tracking Devices and the Fourth Amendment*, 4 U. DENV. CRIM. L. REV. 61, 84–85 (2014) (stating that federal courts seem to treat real-time tracking with increased scrutiny); Theodoric Meyer, *No Warrant, No Problem: How the Government Can Get Your Digital Data*, PROPUBLICA, (June 27, 2014, 10:29 AM), https://www.propublica.org/special/no-warrant-no-problem-how-the-government-can-still-get-your-digital-data (observing a similar trend occurring among state supreme courts). With the arrival of *Riley* this disparate treatment should only increase, *see infra* note 21, Part II.C.3, at least until the role of the third-party doctrine is addressed with respect to location data. *See* Curtis et al., *supra*, at 89–90; Wackman, *supra* note 6, at 300–01.

19. Although exceptions to the warrant requirement make a warrantless search reasonable, this Comment contends that rather than simply extending all exceptions to cover GPS tracking, permissible exceptions should be grounded in the reasoning of *Riley*. *See infra* Part III.D. That is, a court should examine whether the justifications for a given exception are in conflict with the Court's conclusions regarding the unique privacy issues and decreased law enforcement need implicated in searches of smart phones. *Riley* itself did not endorse wholesale application of all warrant exceptions and the language of the opinion clearly suggests a limiting principle. *Riley*, 134 S. Ct. at 2494 (opining that case-specific warrant exceptions "*may* still justify a warrantless search" of a cell phone (emphasis added)). This limiting principle also supports the argument that *Riley* creates a *per se* rule. It would be strange for the Court to conclude that warrant exceptions might apply to future cases involving searches of a cell phone's contents, if *Riley*'s holding was indeed limited to declining to extend one exception to such searches.

20. This includes extensive discussion of *State v. Subdiaz-Osorio*—a recent case from the Wisconsin Supreme Court that came out immediately after *Riley* and discusses the applicability of that decision at some length. The decision generated six writings (out of seven justices) with much of the disagreement stemming from the applicability of *Riley*. *See generally State v. Subdiaz-Osorio*, 849 N.W.2d 748 (Wis. 2014).

analyzes the different warrant exceptions that could justify a search, using the reasoning of *Riley* to guide this inquiry. It argues that of the traditional warrant exceptions, *Riley* expressly permits an exception for exigent circumstances, and that a few others, such as the inevitable discovery rule, could also justify a search. Significantly, Part III argues that one of the exceptions most frequently invoked by courts, the third-party doctrine,[21] should not apply to real-time GPS tracking.

Finally, this Comment concludes by proposing that the Supreme Court should squarely address this issue to provide clarity to lower federal and state courts. Given the Court's underlying reasoning, the Court should extend *Riley*'s bright-line rule to GPS tracking. In the interim, state legislatures and courts should revisit recent decisions and statutes on this issue to address any nonconformities to the (for now) implicit constitutional requirements.[22]

I. FOURTH AMENDMENT JURISPRUDENCE APPLICABLE TO GPS TRACKING

Real-time GPS tracking of a cell phone involves remotely accessing data stored both within the phone and with a wireless carrier—which raises the question of whether such access is cognizable as a search under the Fourth Amendment.[23] Generally, law enforcement must obtain a warrant prior to a search unless an exception to the warrant

---

21. Wackman, *supra* note 6, at 301 ("[T]he third-party doctrine has been the most popular and debated method for law enforcement to access historical cellular location information without a warrant . . . ."); *see* Curtis et al., *supra* note 18, at 87 (discussing use of the third-party doctrine as a common approach courts take to resolve cases involving warrantless tracking).

22. *See, e.g.*, WIS. STAT. § 968.373 (2013–14). Congress recently held hearings on the "Geolocation Privacy and Surveillance (GPS) Act," which would require police to obtain a warrant before tracking and before a phone company could release GPS information. Julian Hattem, *Lawmakers Push to Require a Warrant for GPS Tracking by Police*, THE HILL (Jan. 22, 2015, 5:29 PM), http://thehill.com/policy/technology/230466-lawmakers-roll-out-gps-privacy-bill.

23. The Fourth Amendment lays out dual requirements of reasonableness and probable cause before a search or a seizure may take place, providing in part: "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause . . . ." U.S. CONST. amend. IV. The Court's latest Fourth Amendment case stated that "the ultimate touchstone of the Fourth Amendment is 'reasonableness.'" *Heien v. North Carolina*, 135 S. Ct. 530, 536 (2014) (quoting *Riley*, 134 S. Ct. at 2482). The back and forth between (1) reasonableness as requiring a warrant or exception and (2) a general—independent—reasonableness requirement helps to explain why it is so difficult to discern whether a warrant is required in a given case. *Compare id.*, *with Riley*, 134 S. Ct. at 2482 (describing reasonableness as requiring a warrant or exception). *See also* 3 WAYNE R. LAFAVE, SEARCH AND SEIZURE § 5.2(b) n.15 (5th ed. 2012).

requirement applies.[24] Thus, in the context of GPS tracking outside of the home and without a physical trespass, the threshold inquiry is whether a search has occurred.[25] This Part discusses the technological aspects of GPS tracking and applicable Fourth Amendment standards for determining whether accessing GPS data constitutes a search.

A. GPS Tracking in General

While a complete discussion of how the Global Positioning System (GPS) works is beyond the scope of this Comment,[26] the following description of the process by which a cell phone establishes its location demonstrates that data is in fact sent and received by the device.[27] Cellular GPS tracking works by synching a phone's estimated location, relative to cell towers and wireless networks,[28] with the information received by the phone's GPS system.[29] The in-phone GPS generally

---

24. *See* U.S. CONST. amend. IV; *Riley*, 134 S. Ct. at 2482; *Johnson v. United States*, 333 U.S. 10, 13–15 (1948). The Supreme Court's jurisprudence illustrates the struggle the Court has had with the two clauses—using a reasonableness standard to determine whether a search has in fact occurred, while maintaining the broad warrant requirement. As is often posited, the warrant requirement is perhaps best defined by its exceptions. *See* LAFAVE, *supra* note 23, § 5.2(b).

25. *E.g.*, *State v. Subdiaz-Osorio*, 849 N.W.2d 748, 762–63 (Wis. 2014).

26. For a more thorough description, see GREGORY T. FRENCH, UNDERSTANDING THE GPS: AN INTRODUCTION TO THE GLOBAL POSITIONING SYSTEM: WHAT IT IS AND HOW IT WORKS (1996). The technology was also recently highlighted before Congress. *Geolocational Privacy and Surveillance (GPS) Act: Hearing on H.R. 2168 Before the Subcomm. on Crime, Terrorism, and Homeland Sec. of the H. Comm. on the Judiciary*, 112th Cong. 1 (2012).

27. *See infra* note 28 and accompanying text. Although this overview demonstrates that real-time GPS tracking actually "accesses" data stored within the physical confines of the phone, this distinction should not affect the result under *Riley*. As discussed in Part II, whether real-time location-based tracking is conceptualized as tapping into information stored *physically* within the phone or accessing data requested by and sent to the wireless company (at the behest of law enforcement), the warrantless access implicates the same privacy interests that activated the Court. *See infra* Part II.C.3. Moreover, the Court specifically addressed the difficulties of determining what specific pieces of cellular "data" are actually stored on the phone versus information in transit or within the "cloud." *See infra* notes 134–36 and accompanying text.

28. *See* Paul A. Zandbergen, *Accuracy of iPhone Locations: A Comparison of Assisted GPS, WiFi and Cellular Positioning*, 13 TRANSACTIONS GIS 5, 6–8, 11–13 (2009). One of the problems with new technology is that not all phones determine location in precisely the same way. *See id.* at 6. However, to maximize battery life, modern smart phones typically use the form of "Assisted GPS" (A-GPS) discussed by Zandbergen or a hybrid form which pulls location information from wireless and cellular networks. *See id.* at 6, 12–13. This Comment's discussion of GPS generalizes its discussion of GPS tracking to refer to the hybrid form. *See id.* at 12–13.

29. *See id.* at 6, 12; *see also* Adam Koppel, Note, *Warranting a Warrant: Fourth Amendment Concerns Raised by Law Enforcement's Warrantless Use of GPS*

works by receiving several signals generated by satellites, often "assisted" by a central server, and using those signals to approximate its location.[30]

It is at this point that the phone figures out where it is and displays that information to the user when requested.[31] The cell phone in turn transmits its signal to the phone company.[32] The signal is then received by a centralized database where sequences from particular devices can be used to compile real-time location, travel history, and even rate of speed.[33] Alternatively, the cellular provider may activate the GPS device remotely by signal transmission.[34]

B. Applicable Fourth Amendment Jurisprudence

The Supreme Court has not yet confronted the issue of the warrantless, remote[35] tracking of a suspect by GPS technology. In order to understand the proposed standard, it is necessary to examine the line of cases in which the Court balances the right to privacy against law enforcement interests to determine whether there has been a search.

---

and Cellular Phone Tracking, 64 U. MIAMI L. REV. 1061, 1063–69 (2010); McLaughlin, *supra* note 1, at 426; Patrick Bertagna, *How Does a GPS Tracking System Work?,* EE TIMES (Oct. 26, 2010, 1:25 PM), http://www.eetimes.com/document.asp?doc_id=1278363.

30. Zandbergen, *supra* note 28, at 6–7. With A-GPS most of the satellite communication is performed by a remote server. *Id.* at 6. The phone's GPS communicates with those "satellites that are visible" and "transfer[s] . . . information to the location server over the cellular network." *Id.*

31. *See* Bertagna, *supra* note 29; Stephen Lawson, *Ten Ways Your Smartphone Knows Where You Are*, PCWORLD (Apr. 6, 2012, 6:00 AM), http://www.pcworld.com/article/253354/ten_ways_your_smartphone_knows_where_you_are.html.

32. Zandbergen, *supra* note 28, at 6, 12–13.

33. *Id.* at 6; Bertagna, *supra* note 29.

34. *See, e.g.*, *Sprint Family Locator*, SPRINT, https://sprint-locator.safely.com/welcome.htm (last visited Oct. 2, 2015) [hereinafter *Sprint Locator*]; *see generally* Bertagna, *supra* note 29. Phone companies and third parties often offer lost- or stolen-phone tracking apps that work by locating the phone remotely through GPS. *See* Kay Tan, *10 Useful Apps to Recover a Lost or Stolen iPhone*, HONGKIAT, http://www.hongkiat.com/blog/apps-to-recover-stolen-lost-iphone/ (last visited Feb. 25, 2015). And both articles and cases reveal that companies engage in the practice of locating a phone when requested to do so by law enforcement. *See* Meyer, *supra* note 18 (discussing how Sprint and AT&T reported that they provided location data to U.S. law enforcement 67,000 and 77,800 times in 2012 respectively); *see also State v. Tate*, 849 N.W.2d 798, 803–04 (Wis. 2014); *State v. Subdiaz-Osorio*, 849 N.W.2d 748, 755–57 (Wis. 2014).

35. That is, GPS tracking without the physical attachment of a tracking device. *Cf. United States v. Jones*, 132 S. Ct. 945, 949 (2012) (GPS tracking with physical attachment).

This line of jurisprudence helps explain the process of parsing *Jones*'s GPS tracking dicta with the statements in *Riley*.

1. NONTRESSPASSORY SEARCHES AND THE EXPECTATION OF PRIVACY

The seminal case is *Katz v. United States*.[36] The issue in *Katz* was whether the attachment by law enforcement of an electronic listening device to a public phone booth in order to overhear the defendant's conversations constituted a search.[37] In holding that it did, the Court opined that the Government's activities "violated the privacy upon which [the defendant] justifiably relied while using the telephone booth and thus constituted a 'search and seizure' . . . ."[38]

Two other cases, while not dealing with cell phones, applied *Katz* to electronic tracking in the absence of a trespass.[39] In *United States v. Knotts*,[40] the Court concluded that the surveillance did not implicate the Fourth Amendment,[41] reasoning that law enforcement accomplished most of the surveillance and tracking by following and observing the defendant's car on public roads where an individual "has no reasonable expectation of privacy."[42] By contrast, the Court's decision in *United States v. Karo*[43] concluded that a search occurred when law enforcement used an electronic monitor to locate the house where the defendant had taken the monitored container[44] because of the expectation of privacy one has in not being monitored in the home.

---

36. 389 U.S. 347 (1967).

37. *Id.* at 348–49.

38. *Id.* at 353. The Court found the government's arguments that there can be no search without a physical attachment unconvincing stating, "the 'trespass' doctrine [from previous decisions] can no longer be regarded as controlling." *Id.* The test that emerged from *Katz* is that a search occurs when a person has an "actual (subjective) expectation of privacy . . . that society is prepared to recognize as 'reasonable.'" *Id.* at 361 (Harlan, J., concurring).

39. *United States v. Karo*, 468 U.S. 705 (1984); *United States v. Knotts*, 460 U.S. 276 (1983). Both involved the warrantless attachment by law enforcement of radio transmitters to the inside of containers sold to the defendants, who were using the contents of the containers to manufacture a controlled substance. *Karo*, 468 U.S. at 708; *Knotts*, 460 U.S. at 278–79. Though there was a warrant in *Karo*, it was uncontested on appeal that the warrant was invalid. 468 U.S. at 710.

40. 460 U.S. 276 (1983).

41. *Id.* at 285.

42. *Id.* at 281.

43. 468 U.S. 705 (1984).

44. *Id.* at 714–15 (emphasizing the government had not maintained visual surveillance on the suspects and that the affidavit in support of the warrant specifically relied on the tracking of the transmitter to ascertain the location). The Court ultimately concluded that notwithstanding the defective portions of the affidavit in support of the warrant, there was sufficient probable cause to support it and therefore the search was

2. SEARCHES INVOLVING A PHYSICAL TRESPASS

In *Jones*, the Court addressed the constitutionality of the government's warrantless attachment of a GPS tracking device to an individual's car.[45] Desiring to avoid a broad pronouncement concerning GPS tracking, the Court disposed of the case by returning to the common-law trespass analysis repudiated in *Katz*.[46] The Court held that a search occurs whenever the government commits a common-law physical trespass.[47] Justice Alito, joined by three members of the Court, concurred in the judgment on the grounds that, under *Katz*, the length of the GPS tracking violated the defendant's reasonable expectation of privacy.[48] Addressing this approach, Justice Scalia stated in dicta that the proper standard of analysis in GPS tracking when no attachment occurs would be the reasonable expectation of privacy test.[49]

3. SEARCH INCIDENT TO ARREST AND *RILEY V. CALIFORNIA*

The search-incident-to-arrest doctrine is an exception to the general warrant requirement that permits police to search through articles within a criminal suspect's immediate area of control. The doctrine stems from a long history at English common law of recognizing "the right on the part of the Government . . . to search the person of the accused when legally arrested to discover and seize the fruits or evidences of crime."[50] Under this exception, the Court has held it permissible to search a cigarette packet carried by the defendant[51] and the glove compartment of

---

valid. *Id.* at 719–21. A similar conclusion was reached by the Wisconsin Supreme Court in *State v. Tate*, a case involving cell phone tracking. *State v. Tate*, 849 N.W.2d 798, 809–10 (Wis. 2014) (determining that there was a sufficient factual basis for the magistrate to find probable cause despite the deficiencies in the warrant).

45. *United States v. Jones*, 132 S. Ct. 945, 948 (2012).

46. *See id.* at 949–52; *supra* note 38 and accompanying text.

47. *Jones*, 132 S. Ct. at 949–50, 953 n.8. This *per se* rule exists in other Fourth Amendment contexts, such as when police seek to enter a home. However, it is just as easy to conceptualize the cases adopting such *per se* holdings—that an unreasonable search has occurred—as being grounded in the idea that the privacy interests are so great in the specific context that there is no need to balance those interests against the interests of law enforcement. *See Riley v. California*, 134 S. Ct. 2473, 2488 (2014).

48. *Jones*, 132 S. Ct. at 964 (Alito, J., concurring).

49. *Id.* at 953; *see, e.g.*, *United States v. Knotts*, 460 U.S. 276, 281, 285 (1983).

50. *Weeks v. United States*, 232 U.S. 383, 392 (1914).

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

an arrestee's vehicle,[52] but has held it impermissible for officers to search the entirety of a home.[53]

The traditional justifications for the exception are twofold. First, there is a concern for officer safety, as the arrestee's immediate area of control could contain weapons that the arrestee could use against law enforcement.[54] Second, the doctrine permits law enforcement to discover evidence of illegal activities, which an arrestee might otherwise attempt to destroy.[55] Finally, in discussing *United States v. Robinson*,[56] *Riley* offered another justification which follows from the traditional ones: when officers establish probable cause to arrest, the privacy interests of an arrestee in any personal property located on his or her person are considerably diminished.[57] As modern era courts assess the reasonableness of a search by balancing the degree of individual privacy interests against the degree "to which [the search] is needed for the promotion of legitimate governmental interests[,]"[58] (e.g., officer safety and preservation of evidence) these diminished privacy interests tilt the balance in favor of the government.[59]

With these traditional justifications in mind, the Court in *Riley* analyzed whether the rationale behind search incident to arrest could extend to searches of the digital contents of one's cell phone.[60] The Court agreed with the lower court's conclusion that the officers, in searching the phone, "knew exactly what they would find therein: data."[61] Furthermore, the officers "also knew that the data could not harm them."[62] As to the prevention of the destruction of evidence, the Court offered numerous solutions such as securing the phone and

---

52. *Arizona v. Gant*, 556 U.S. 332, 343 (2009) (stating that passenger compartment searches are reasonable only when the arrestee is unsecured and within reach at the time of the search).

53. *See Chimel v. California*, 395 U.S. 752, 753–54, 768 (1969).

54. *Id.* at 763.

55. *Id.*; *see supra* note 50 and accompanying text.

56. 414 U.S. 218 (1973).

57. Privacy interests are diminished as the defendant will be incarcerated and his property held by law enforcement, often while the prosecution seeks a warrant to search the property seized. *See Riley v. California*, 134 S. Ct. 2473, 2485 (2014).

58. *Id.* at 2484 (quoting *Wyoming v. Houghton*, 526 U.S. 295, 300 (1999)).

59. *See id.* at 2488 (reasoning that the justifications for the exception illustrate the heightened government interests while the privacy interests are reduced by the arrestee's custodial status).

60. *Id.* at 2488, 2492.

61. *Id.* at 2485 (quoting *United States v. Wurie*, 728 F.3d 1, 10 (1st Cir. 2013)).

62. *Id.*

obtaining a warrant to go through its contents and covering the phone or removing the battery in order to prevent remote wiping.[63]

In short, the Court concluded that the privacy interests in a cell phone outweigh the justifications underlying the exception.[64] This was true in spite of "an arrestee's reduced privacy interests upon being taken into police custody."[65] As discussed below, there are two other contexts where the Court has held that privacy interests are so great as to render warrantless searches *per se* unreasonable: searches of the home and searches by physical trespass.[66] Elevating cell phone data into these categories signals that the Court may be embracing the immense privacy interests that these devices carry, as well as the interpretive problems and personal liberty implications that would result from assessing such searches under a reasonableness analysis.

II. *RILEY* APPLIES TO SEARCHES OF A CELL PHONE'S GPS LOCATION DATA

Multiple interpretations of *Riley* have emerged, and while there are (at least) two ways to read the decision, this Part contends that the Court's methodology naturally supports a broader application. On a narrow reading, *Riley* merely carves out an exception which prevents the government from relying on the search-incident-to-arrest doctrine to search a cell phone.[67] Under a broader reading, *Riley* applies to searches of cell phone data in any context,[68] or at the very least is conclusive

63. *Id.* at 2486–88.

64. And therefore greater than the government's interests in the warrantless search. *See id.*

65. *Id.* at 2488.

66. *See supra* notes 8, 47 and accompanying text.

67. *E.g.*, *United States v. Figueroa*, No. 12 Cr. 233 (ALC), 2014 U.S. Dist. LEXIS 146722, at *16–17 (S.D.N.Y. Oct. 1, 2014). In *Figueroa*, the court held that *Riley* was narrowly limited and only applied to a search of a cell phone incident to arrest. *Id.* at *17. Therefore, the court concluded that a cell phone found in the defendant's car could be searched as the officer had probable cause to search the vehicle. *Id.* at *15 (reasoning that because the officer "had probable cause to believe the Defendant's vehicle contained evidence of a crime[,] . . . a warrantless search of the cell phone recovered from the vehicle was reasonable under the Fourth Amendment in accordance with the automobile exception."); *accord* Leslie A. Shoebotham, *The Strife of* Riley*: The Search-Incident Consequences of Making an Easy Case Simple*, 75 LA. L. REV. 29, 40–41 (2014) (discussing the fear that *Riley* would cause courts to disconnect the vehicle search exception articulated in *Arizona v. Gant* from the justifications for search incident to arrest); *see Arizona v. Gant*, 556 U.S. 332, 344 (2009).

68. *E.g.*, *United States v. Stile*, 1:11-cr-00185-JAW, 2014 U.S. Dist. LEXIS 144241, at *10 (D. Me. Oct. 10, 2014). In *Stile*, the court examined the reasoning in *Riley* and speculated that it applies to all searches of cell phones. *Id.* at *10

evidence that society has recognized an objectively reasonable expectation of privacy in one's cell phone location.[69] This growing divide in how courts interpret and apply *Riley* highlights the need to clarify the role of the Fourth Amendment with respect to location-based tracking of cell phones.[70]

To support a broader reading of *Riley*, several points will be established: (1) *Riley* contains, as part of its holding, language supporting this position; (2) the policy concerns discussed by the Court support the broader reading; and (3) tracking a phone by GPS actually results in law enforcement accessing the phone's data (thereby bringing the tracking within the literal scope of *Riley*'s holding). Therefore, *Riley*, rather than *Jones*, should be read to control the issue of whether a search occurs during cellular GPS tracking. *Jones* makes only a general statement regarding GPS searches without a physical trespass, whereas *Riley* explicitly requires a warrant for searching a cell phone's data.[71]

A. The Two Readings of Riley

One way to interpret *Riley* is that the decision is limited to cell phone searches which occur during an arrest.[72] Courts taking this view

("[Although] the extent to which *Riley* would be extended to a residential search not incident to arrest is not precisely known . . . the Court assumes that *Riley would apply to a search not* incident to arrest." (emphasis added)).

69. That is, that *Katz*'s second prong is met. *See, e.g.*, *Hedgepath v. Commonwealth*, 441 S.W.3d 119, 129 (Ky. 2014) ("[*Riley*] held that there is a reasonable expectation of privacy in the contents of one's cell phone."); *Tracey v. State*, 152 So. 3d 504, 524–26 (Fla. 2014). In *Tracey*, the Florida Supreme Court concluded that although *Riley* did not address GPS tracking of a cell phone, Sotomayor's concurrence in *Jones* together with the unanimity of *Riley* tipped the scales of the expectation of privacy test in favor of finding the warrantless tracking unconstitutional. *See id.* at 512, 515, 524–26; *accord* Lamparello & MacLean, *supra* note 8, at 39 ("*Riley*'s reasonableness standard . . . recognized a generalized expectation of privacy in cell phone data . . . .").

70. Decisions from state supreme courts and lower federal courts confronting GPS tracking after *Riley* reveal the need for a bright-line rule. These cases reveal a range of approaches and indicate that there is no consensus on the proper standard for analyzing either real-time or historic location-data-based tracking. *See supra* notes 67–69; *infra* notes 72–82.

71. *Compare United States v. Jones*, 132 S. Ct. 945, 952 (2012), *with Riley v. California*, 134 S. Ct. 2473, 2485 (2014).

72. *See, e.g.*, *Figueroa*, 2014 U.S. Dist. LEXIS 146722, at *15–17. This reading is problematic for two reasons. First, it ignores the principal justification for the Court's holding in *Riley*—searches of cell phones are unreasonable because of the vast amount of private data that the devices contain. *See Riley*, 134 S. Ct. at 2489. And second, while the issue in *Riley* was search incident to arrest, the Court held that there was a general requirement of a warrant before searches of cell phone data would be

have upheld warrantless searches of a cell phone when supported by probable cause,[73] mentioned in a general warrant without a description of the data to be searched,[74] or when limited merely to the phone's exterior.[75] Cases have also upheld searches when based on an exception to the warrant requirement, such as consent,[76] the border search exception,[77] or an exigent circumstance.[78]

A second way to read the decision is that *Riley* creates a general requirement that police obtain a warrant before searching a defendant's cell phone. Interpreted this way, the rule would apply beyond situations where authorities have seized the defendant's personal effects pursuant to an arrest.[79] This interpretation would reach the question of GPS tracking.[80] The explicit exception to this rule is that exigent

---

permissible. *Id.* at 2485. Somewhat ironically, the *Figueroa* court repeated this point. *Figueroa*, 2014 U.S. Dist. LEXIS 146722, at *14. Nevertheless, the court proceeded to apply a probable cause non-exigency exception in upholding the search. *Id.* at *14–15 (applying the automobile exception).

73. *See Figueroa*, 2014 U.S. Dist. LEXIS 146722, at *15.

74. *Compare Hedgepath*, 441 S.W.3d at 129–31 (taking a broad view of *Riley* but nevertheless upholding a search where the warrant listed a cell phone as one of the things to be searched within the defendant's home without specifying the data to be searched), *with State v. Henderson*, 854 N.W.2d 616, 632–34 (Neb. 2014) (voiding on particularity grounds a warrant to search "any and all" content on the defendant's cell phone).

75. *United States v. Adekoya*, 60 F. Supp. 3d 287, 293–94 (D.N.H. 2014) (concluding *Riley* did not prevent law enforcement from viewing the serial number on a phone's exterior without a warrant).

76. *United States v. Bailey*, No. 2:14-cr-121, 2014 U.S. Dist. LEXIS 154482, at *18–20 (E.D. Va. Oct. 30, 2014). The court in *Bailey* held that *Riley* did not "[impose] a blanket rule requiring a warrant for all searches of cell phones without exception," but rather "incorporate[d] existing exceptions to the warrant requirement along with the warrant requirement itself." *Id.* at *18 n.7.

77. *See United States v. Saboonchi*, 48 F. Supp. 3d 815, 818–19 (D. Md. 2014). It would be incorrect to read *Saboonchi* as advocating for the narrow reading however. The court explained that *Riley*'s concerns with conventional searches also applied to remote, forensic searches and concluded that the same logic extended beyond the cell phone context to other containers of digital information (such as computers). *Id.* at 819. However, the court nevertheless applied the traditional reasonable-suspicion border-exception standard in upholding the warrantless search. *Id.* at 819–20.

78. *See State v. Subdiaz-Osorio*, 849 N.W.2d 748, 768 (Wis. 2014).

79. *See, e.g.*, *United States v. Stile*, No. 1:11-cr-00185-JAW, 2014 U.S. Dist. LEXIS 144241, at *10–12 (D. Me. Oct. 10, 2014).

80. This view was articulated in *Subdiaz-Osorio* in Justice Crooks' concurring opinion. *Subdiaz-Osorio*, 849 N.W.2d at 776 (Crooks, J., concurring) ("The [holding] of the United States Supreme Court in [*Riley*] . . . lead[s] me to the conclusion that, absent case-specific exceptions . . . a warrant is required for the search of a cell phone's location."). Currently, Justice Crooks' statement is among the strongest support (in the GPS tracking context) for the broader reading, but other high courts have adopted similar views. *See Tracey v. State*, 152 So. 3d 504, 524–26 (Fla. 2014).

circumstances may justify searching a phone without a warrant.[81] Implicitly, *Riley* suggests "other case-specific exceptions *may* still justify a warrantless search" of a cell phone.[82]

B. Support for the Broader Reading

Many of the cases taking a narrow view of *Riley* ignore the vast storage capacity that cell phones have, frustrating the qualitative differences that the Court saw between these devices and other articles.[83] Indeed, recent opinions appear to agree that *Riley* generally requires a warrant for searching a cell phone.[84] Therefore, while it may be tempting to give *Riley* a narrow reading to preserve law enforcement flexibility in a developing area of the law,[85] the broader interpretation is on firmer ground for two reasons. First, the language of the opinion supports extension of the rule beyond search incident to arrest.[86]

---

81. *Riley v. California*, 134 S. Ct. 2473, 2494 (2014) ("In light of the availability of the exigent circumstances exception, there is no reason to believe that law enforcement officers will not be able to address some of the more extreme hypotheticals that have been suggested . . . .").

82. *Id.* (emphasis added). The limiting principle as to the permissible exceptions from *Riley*'s holding provides additional support for a broad reading. *See supra* note 19.

83. *See Riley*, 134 S. Ct. at 2489–91.

84. *See, e.g.*, *Stile*, 2014 U.S. Dist. LEXIS 144241, at *10–11; *United States v. Ulbricht*, No. 14-cr-68 (KBF), 2014 U.S. Dist. LEXIS 145553, at *26–27 (S.D.N.Y. Oct. 10, 2014) ("[T]the Court [in *Riley*] determined that warrants are generally required to search the contents of cell phones."); *United States v. Saboonchi*, 48 F. Supp. 3d 815, 819–20 (D. Md. 2014); *Smith v. State*, 770 S.E.2d 610, 614 n.4 (Ga. 2015) ("[E]xcept under exigent circumstances or other case-specific exceptions, the warrantless search of a cell phone is unconstitutional."); *Hedgepath v. Commonwealth*, 441 S.W.3d 119, 130 (Ky. 2014) ("[*Riley*] concluded, the contents of a cell phone are not subject to a warrantless search . . . ."). *But see United States v. Figueroa*, No. 12 Cr. 233 (ALC), 2014 U.S. Dist. LEXIS 146722, at *14–15 (S.D.N.Y. Oct. 1, 2014). Recent commentary also agrees with this point. *See* Shoebotham, *supra* note 67, at 33 & n.14; Charles D. Weisselberg, *Cell Phones and Everything Else: Criminal Law Cases in the Supreme Court's 2013–2014 Term*, 50 SUP. CT. REV. 164, 165 (2014); Robert Barnes, *Supreme Court Says Police Must Get Warrants for Most Cellphone Searches*, WASH. POST (June 25, 2014), http://wpo.st/T5Hi0; Richard M. Re, *Symposium: Inaugurating the Digital Fourth Amendment*, SCOTUSBLOG (June 26, 2014, 12:37 PM), http://www.scotusblog.com/2014/06/symposium-inaugurating-the-digital-fourth-amendment. However, the scholarly agreement is far from unanimous. *See, e.g.*, Wackman, *supra* note 6, at 263 (concluding that the Fourth Amendment is not implicated when law enforcement accesses *historical* cell site location data).

85. *See* Ganz, *supra* note 9, at 1327 (discussing how law enforcement benefits from GPS tracking).

86. Courts taking the narrow reading emphasize that *Riley* stated the issue before the court as "whether the police may, without a warrant, search digital information on a cell phone seized from an individual who has been arrested." *Riley*,

Second, refusing to require a warrant would frustrate the Court's concerns, discussed in *Jones* and *Riley*, regarding cell phone data and GPS.

1. THE LITERAL HOLDING OF *RILEY* SUPPORTS THE BROADER READING

The *Riley* Court explicitly stated its holding:

> Our holding, of course, is not that the information on a cell phone is immune from search; it is instead that *a warrant is generally required* before such a search, *even when a cell phone is seized incident to arrest*. Our cases have historically recognized that the warrant requirement is "an important working part of our machinery of government," not merely "an inconvenience to be somehow 'weighed' against the claims of police efficiency."[87]

The Court's conclusion—that a warrant is required "even when" a cell phone is seized pursuant to the exception—carries two implicit assumptions. First, accessing information on a cell phone must generally be a search under *Katz*, because a warrant is only ever required when an intrusion rises to the level of a search. Second, requiring a warrant, notwithstanding the presence of an exception (i.e., search incident to arrest), implies that not all exceptions will make the warrantless search of a phone reasonable.[88]

---

134 S. Ct. at 2480; *see, e.g.*, *Figueroa*, 2014 U.S. Dist. LEXIS 146722, at *17 ("*Riley*'s calculated language aimed at separating the legal standard and underlying rationale of *Gant* signals that its holding is limited to a search of a cell phone incident to arrest."); *State v. Carle*, 337 P.3d 904, 910 n.6 (Or. Ct. App. 2014) ("The Court in *Riley* noted that, '[b]ecause the United States and California agree that [the two consolidated cases before the Court] involve *searches* incident to arrest, these cases do not implicate the question whether the collection or inspection of aggregated digital information amounts to a search under other circumstances.'" (alteration in original) (quoting *Riley*, 134 S. Ct. at 2489 n.1)).

87. *Riley*, 134 S. Ct. at 2493 (emphasis added) (quoting *Coolidge v. New Hampshire*, 403 U.S. 443, 481 (1971)).

88. Said another way, a search is unreasonable unless there is a warrant or an exception to make it reasonable, a warrantless search of a cell phone is generally unreasonable, and not all exceptions to the warrant requirement will make the search of a cell phone reasonable. See *Riley*, 134 S. Ct. at 2482, 2494. The Court did not specify what other exceptions might apply, *see id.* at 2494, and courts are divided as to whether an exigency is required or another exception will do. *See supra* notes 72–78 and accompanying text. This issue is discussed more *infra*, in Part III.

2. THE COURT'S CONCERNS WITH BOTH CELLULAR DATA AND GPS TRACKING SUPPORT THE BROADER READING

The principle justification for treating cell phones differently than other articles subject to search incident to arrest is grounded in their vast storage capacity and the privacy interests that attach with such capacity.[89] As previously discussed, the Court made clear that claims of law enforcement efficiency and other law enforcement interests are inferior to these interests.[90] And as explained below, while the interest in location data is different, it is no less substantial.[91]

Admittedly, the other major consideration by the Court—the decreased law enforcement interest—weighs on the other side of the scale and supports the narrow reading. Because the suspect is in custody and the phone is secure in the context of search incident to arrest, police have time to obtain a warrant if one is required.[92] This may not be the case for searches of cellular data in situations involving heightened law enforcement need,[93] or other contexts including GPS tracking.[94] However, the availability of certain warrant exceptions mitigates law enforcement need in those circumstances.[95]

---

89. *See Riley*, 134 S. Ct. at 2488–91; Ruth Bader Ginsburg & Robert A. Stein, *A Conversation Between Justice Ruth Bader Ginsburg and Professor Robert A. Stein*, 99 MINN. L. REV. 1, 25 (2014) (describing Justice Ginsburg's take on the differences in storage capacity between cell phones and other articles of personal property); *see also* Shoebotham, *supra* note 67, at 39–40.

90. *See supra* text accompanying note 87.

91. *See infra* notes 96–99 and accompanying text.

92. *See Riley*, 134 S. Ct. at 2486 ("[The defendants] concede that officers could have seized and secured their cell phones to prevent destruction of evidence while seeking a warrant.").

93. *See, e.g.*, *United States v. Saboonchi*, 48 F. Supp. 3d 815, 819 (D. Md. 2014) (stating that although *Riley* found law enforcement interests diminished in the search-incident-to-arrest context, "*Riley* did not diminish the Government's interests in protecting the border").

94. Lamparello & MacLean, *supra* note 8, at 34; *see also* Ricciuti & Parker, *supra* note 6, at 9; *cf.* Ganz, *supra* note 9, at 1327, 1330–32, 1338–42, 1354–55 (discussing situations with heightened law enforcement need). *Riley* addresses some of those contexts by stating that exigent circumstances may justify a search of a phone's digital contents. *Riley*, 134 S. Ct. at 2494; *see, e.g.*, *United States v. Bailey*, No. 2:14-cr-121, 2014 U.S. Dist. LEXIS 154482, at *18 n.7 (E.D. Va. Oct. 30, 2014).

95. *State v. Subdiaz-Osorio*, 849 N.W.2d 748 (Wis. 2014), discussed *infra* in Part III.C, provides a good example. In *Subdiaz-Osorio*, the police had good reason to believe that the defendant was fleeing the country to relatives in Mexico after committing an alleged homicide, *id.* at 754–55, and obtained his GPS location from his cellular provider. *Id.* at 755–56. The lead opinion for the Wisconsin Supreme Court assumed a search but concluded that the search was not unreasonable, justified under a "fleeing suspect" exigency theory. *Id.* at 752, 769–71.

Moreover, the concerns expressed in *Jones*, demonstrate just how substantial the Court views the privacy interests in location-based searches.[96] Unlike tracking someone's vehicle by attaching a GPS locator or installing a transmitter into a container, tracking an individual's cell phone potentially involves following him or her at all times. Like *Karo* then and in contrast to *Knotts*, law enforcement inevitably will trace a phone to a location where the phone's owner has an indisputable expectation of privacy (e.g., the home).[97] But regardless of whether tracking crosses into the home,[98] the potentially omni-present nature of cell phone tracking brings it squarely within the concerns discussed by Justices Alito and Sotomayor in *Jones*.[99]

Accordingly, while the privacy interests in cellular GPS data are different than those discussed in *Riley*, they are in no way less significant. And while law enforcement need could potentially be greater, the balance of need versus interest is not markedly different, given the availability of exigencies. Finally, it is significant that *Riley* rejected an *ad hoc* approach, instead favoring a clear rule.[100]

C. Riley*'s* Per Se *Rule Applies to Searches of a Cell Phone's GPS*

Setting aside *Jones*'s concurring opinions, one could conclude *Riley* applies beyond search incident to arrest and still conclude that Justice Scalia's majority opinion in *Jones* provides the proper standard, or carves out an exception, for situations where the only cellular data access by law enforcement is GPS data.[101] But however appealing this

---

96. The five concurring justices in *Jones* would have found a search under *Katz*. *United States v. Jones*, 132 S. Ct. 945, 963–64 (2012) (Alito, J., concurring); *see also id.* at 955 (Sotomayor, J., concurring) (adopting the majority's trespass theory by also concluding that a search occurred under *Katz*).

97. *See Tracey v. State*, 152 So. 3d 504, 524 (Fla. 2014) (contending the close proximity people keep to their phones will cause this effect); *supra* notes 41–44 and accompanying text.

98. Of course, if the broad reading of *Riley* controls, then crossing the property-based boundary of the phone, like crossing the boundary of the home, will already render any search unreasonable.

99. *See infra* note 139.

100. The Court stated, "[I]f police are to have workable rules, the balancing of 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.'" *Riley*, 134 S. Ct. at 2491–92 (alterations in original) (quoting *Michigan v. Summers*, 452 U.S. 692, 705 n.19 (1981) (quoting *Dunaway v. New York,* 442 U.S. 200, 219–20 (1979) (White, J., concurring))).

101. *Jones*, 132 S. Ct. at 953 ("Situations involving merely the transmission of electronic signals without trespass would *remain* subject to *Katz* analysis."). *See, e.g.*, *State v. Subdiaz-Osorio*, 849 N.W.2d 748, 764 (Wis. 2014); *Tracey*, 152 So. 3d at 514, 524–26 (Fla. 2014).

doctrinal syllogism is, the broad reading of *Riley* should apply to cellular GPS searches for several reasons.

First, if one accepts that *Riley* holds that a warrant is generally required before police can search a cell phone, whether in an arrest context or otherwise, that holding should control over the dicta in *Jones*.[102] Second, *Riley*'s categorical rule, and the methodology used to arrive at it, is similar to cases where the Court has identified bright-line categories that the Fourth Amendment protects.[103] Within such categories, courts do not undertake a *Katz*-type analysis.[104] Finally, a search of a phone's location by GPS—though not involving attachment—still involves accessing "data" stored on the phone and data generated by the phone and stored on a remote server.[105] The Court in *Riley* agreed with the Government that such accesses of data stored outside of the phone (e.g., in the "cloud") would be impermissible.[106] Therefore, just as the Court refused to conclude that police could access the vast amounts of data in a cell phone seized incident to arrest, so long as they did so remotely,[107] it seems equally counter-intuitive to allow police to access the portions of GPS data held in a server.

1. OTHER CATEGORIES WITH BRIGHT-LINE WARRANT RULES

Fourth Amendment jurisprudence traditionally has protected the articles explicitly mentioned or contemplated by the text of the

---

102. This is true for two reasons. First, the statement in Justice Scalia's opinion in *Jones* was made in response to accusations from Justice Alito's concurrence and is arguably dicta. *See Jones*, 132 S. Ct. at 953–54. Additionally, while *Jones* is the more specific language as to GPS tracking, *Riley* contains the more specific command as to cell phones in general. *Compare id.* at 953, *with Riley*, 134 S. Ct. at 2485. As Fourth Amendment issues in areas of new technology are decided on a "technology by technology" basis, a bright line rule for cell phones should control. McLaughlin, *supra* note 1, at 429; *see Dow Chemical Co. v. United States*, 476 U.S. 227, 238–39 (1986).

103. *E.g.*, *Payton v. New York*, 445 U.S. 573 (1980); *see infra* Part II.C.1.

104. *See, e.g.*, *Dow Chemical*, 476 U.S. at 235–39 (considering whether to apply the "industrial curtilage" *per se* search rule which is related to the *Payton* rule); *id.* at 244 (Powell, J., dissenting) (criticizing the majority for failing to apply *Katz*).

105. *See* Zandbergen, *supra* note 28, at 6; *infra* Part II.C.3.

106. *Riley*, 134 S. Ct. at 2491 ("The [government] concedes that the search incident to arrest exception may not be stretched to cover a search of files accessed remotely—that is, a search of files stored in the cloud."); *see also* Elijah Yip & Martin E. Hsia, *Confidentiality in the Cloud: The Ethics of Using Cloud Services in the Practice of Law*, COMPUTER & INTERNET L., Dec. 2014, at 19, 19.

107. That accessing a GPS involves only a small amount of data is probably the strongest argument against extending *Riley*. However, as will be discussed, the Court rejected suggested rules proposed by the government limiting the amount of data police could access to the previous ten calls or ten text messages. *See Riley*, 134 S. Ct. at 2491–93; *infra* Part II.C.3.

Amendment.[108] Specifically, the Amendment protected against certain government intrusions within certain places.[109] This protection changed in the line of cases emerging from *Katz* in which the Court declared that the Amendment protects the privacy interests of "people, not places."[110] In *Katz* and the cases that followed, the Court created a test to determine whether a search within the meaning of the Amendment had occurred—which required examining the privacy interests the actor had in the specific article or place searched.[111] However, at least within two property-based contexts, the Court continues to apply categorical rules.

The first category involves searches of a defendant's home.[112] In holding that such entries are impermissible, the *Payton* Court noted the old adage that "a man's house is his castle."[113] The Fourth Amendment, the Court noted, protects a person's privacy interest in being able to retreat into the home and enjoy seclusion therein.[114] And in later cases, the Court clarified that *Katz* was not "intended to withdraw any of the protection which the Amendment extends to the home . . . ."[115] In other words, there is no privacy balancing analysis in searches entering the home.

Another historically proscribed form of search was the physical trespass.[116] In *Jones*, the Court concluded that *Katz* and its progeny did not abrogate this physical trespass doctrine and reinstated the trespass analysis as applied to the warrantless physical attachment of a GPS tracking device to the defendant's vehicle.[117] The Court concluded that this was impermissible, even though the defendant was only tracked

---

108. *See supra* text accompanying note 24; *see also* Ric Simmons, *From* Katz *to* Kyllo*: A Blueprint for Adapting the Fourth Amendment to Twenty-First Century Technologies*, 53 HASTINGS L.J. 1303, 1303 (2002).

109. Simmons, *supra* note 108, at 1303–04, 1307–11.

110. *Katz v. United States*, 389 U.S. 347, 351 (1967).

111. *See id.* at 361 (Harlan, J., concurring); *see, e.g.*, *United States v. Karo*, 468 U.S. 705, 714–15 (1984); *United States v. Knotts*, 460 U.S. 276, 285 (1983).

112. *See, e.g.*, *Payton v. New York*, 445 U.S. 573 (1980). *Payton* was decided thirteen years after *Katz* and yet resolved the case with a categorical rule. *See generally id.*

113. *Id.* at 598.

114. *Id.* The Court later made clear that exigent circumstances still provide an exception and permit warrantless entries into the home. This is true even when police create the exigency—at least in the absence of bad faith. *See Kentucky v. King*, 131 S. Ct. 1849, 1860 (2011).

115. *Alderman v. United States*, 394 U.S. 165, 180 (1969) (decided two years after *Katz*).

116. *United States v. Jones*, 132 S. Ct. 945, 949–51 (2012).

117. *Id.* at 948–49. Simmons points out that the Court used property rights language after *Katz* in upholding searches based on a lack of "'physical entry' onto [a] defendant's property." Simmons, *supra* note 108, at 1315–16 (quoting *Dow Chemical Co. v. United States*, 476 U.S. 227, 237 (1986)).

while on public roads, which had previously been held not to violate a reasonable expectation of privacy.[118] The Court's return to the creation of *per se* rules was seen by some as demonstrating a desire—by a majority of the Court—to move away from analyzing searches on a case-by-case basis using *Katz*.[119]

2. USE OF SIMILAR CATEGORICAL REASONING IN *RILEY*

In both *Riley* and the other intrusions with categorical rules, the Court discusses the increased privacy interests that an actor has against the nature of the intrusion committed.[120] And despite their bright-line language, the holdings of these *per se*, property-based cases can be conceptualized as an application of the *Katz* doctrine.[121] Therefore, by establishing a categorical rule for an intrusion as to the specific article of a cell phone, the Court merely brings the intrusion back within the general requirement for a warrant.[122]

3. LOCATING A PHONE BY GPS INVOLVES "ACCESSING" THE DATA STORED ON A PHONE AND THUS IMPLICATES THE BROADER RULE

A cell phone determines its location primarily through the reception of signals emitted from satellites and cell towers.[123] Based on this, one could conclude that tracking a suspect by viewing the phone's GPS location does not actually implicate accessing data stored on the phone.[124] In line with this thinking, some decisions have examined a

---

118. *See United States v. Knotts*, 460 U.S. 276, 283–88 (1983).

119. *See generally* Orin S. Kerr, *The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution*, 102 MICH. L. REV. 801, 809–15 (2004); Simmons, *supra* note 108, at 1314–21. *Cf.* F. LAWRENCE STREET, LAW OF THE INTERNET, ch.2, § 2.03(2a) (Matthew Bender ed., 2014) (discussing the Court's Fourth Amendment cases between *Jones* and *Riley* and opining that, in those intervening decisions, "the Court moved away from property ideas of privacy to expectation ideas").

120. *See Riley v. California*, 134 S. Ct. 2473, 2484 (2014); *Jones*, 132 S. Ct. at 949–51; *Payton v. New York*, 445 U.S. at 596 n.43, 596–600 (1980).

121. Specifically, if *Katz* is the test to determine whether a search has occurred in the first place, then all the Court is doing by establishing *per se* rules within certain types of intrusions is determining that the specific privacy interest at issue necessarily meets the standard. *See generally* Lamparello & MacLean, *supra* note 8, at 33.

122. *Riley*, 134 S. Ct. at 2482–85. *Riley*'s characterization of the warrant requirement provides further support for this conclusion—that is, a warrantless search "is reasonable only if it falls within a specific exception to the warrant requirement." *Id.* at 2482; *see supra* note 15 and accompanying text.

123. *See* Zandbergen, *supra* note 28, at 6, 11–13; *see also supra* Part I.A.

124. *Cf. State v. Subdiaz-Osorio*, 849 N.W.2d 748, 784 (Wis. 2014) (Ziegler, J., concurring) (opining that "[t]he location of a cell phone [as opposed to] the contents

defendant's cell phone contract and used clauses—in which providers state that they will release GPS information to law enforcement—as evidence that the defendant did not have a subjective expectation of privacy under *Katz*.[125] However, the idea that GPS location tracking does not involve a search or access of the data actually stored on the phone is erroneous because it misunderstands the technology, is factually inaccurate, and ignores much of the language in *Riley*.

First, from a technical standpoint, the modern "smart phone" determines its location by comparing the GPS signals received by a remote server and its internal GPS with its distance from cell phone towers, wireless networks, and other geographical sources.[126] Moreover, one of the ways that a cell phone is able to determine its location so quickly is by using previous determinations of location—stored as data on the device[127]—to narrow down its search. Essentially the phone begins with an assumption that it is closer to, rather than farther from, the last place that it was.[128] The "memory" of those previous locations is clearly data stored within the phone.[129]

Second, because the GPS tracking of a phone requires use of previous location data stored within the phone, it is factually inaccurate

---

contained therein may or may not be subject to the same constitutional analysis" used in *Riley*).

125. *See, e.g.*, *id.* at 783–84 (Roggensack, J., concurring); *see also Sprint Corporation Privacy Policy*, SPRINT, http://www.sprint.com/legal/privacy.html/ (last updated May 2, 2014). Although Justice Roggensack's concurrence would have resolved the case using the cell phone contract, Justice Prosser stated in the lead opinion that he was "reluctant to say that a person loses his reasonable expectation of privacy based on an opaque contract" and that "[t]he Fourth Amendment is complicated enough without introducing contract interpretation into the calculus." *Subdiaz-Osorio*, 849 N.W.2d at 765–66. The lead opinion also concluded that, even if clear, the contract only governed the conduct of the cell phone company and that to find otherwise would "[invite] law enforcement to be complacent in its requests for tracking." *Id.* at 766.

126. *See* Zandbergen, *supra* note 28, at 6, 12–13; Bertagna, *supra* note 29.

127. *See* Zandbergen, *supra* note 28, at 12–13; Lawson, *supra* note 31. A smart phone might also be programmed to assume that it is in a location where it frequently locates itself. For example if the phone determined that it was in Madison, Wisconsin the last 100 times the GPS was activated, the phone could begin its search there. *See generally* Lawson, *supra* note 31.

128. This is one possible reason why it takes a cell phone so long to figure out its location upon arriving in a new city—A-GPS requires an initial download from a remote server or directly from a satellite as to where the GPS satellites are and will be for the next couple hours. *See* Lawson, *supra* note 31; *see generally* Zandbergen, supra note 28, at 6.

129. *Cf.* Melissa Ulbrict, *How to Remove Location Information from Mobile Photos*, IDEA LAB (Feb. 28, 2011), http://www.pbs.org/idealab/2011/02/how-to-remove-location-information-from-mobile-photos055/ (discussing an analogous situation with respect to how location data is often attached to photos).

to view such tracking as merely the collection of voluntarily broadcasted location information.[130] In addition, law enforcement often tracks a cell phone's GPS by going directly to the phone company and requesting that *the company determine* where the device is located.[131] This reverse locating can be conceptualized as involuntarily forcing the phone to determine its location, and such a determination necessarily involves a comparison to previous locations stored within the phone and GPS information communicated to the remote server.[132] Plainly then, the data of the cell phone is accessed in conducting such tracking.[133]

Moreover, *Riley* addressed the contention that the data accessed is being broadcasted beyond the storage space contained within the phone and is therefore not "accessed"[134]:

> To further complicate the scope of the privacy interests at stake, the data a user views on many modern cell phones may not in fact be stored on the device itself. . . .
>
> The United States concedes that the search incident to arrest exception may not be stretched to cover a search of files accessed remotely—that is, a search of files stored in the cloud. . . . [O]fficers searching a phone's data would not typically know whether the information they are viewing was stored locally at the time of the arrest or has been pulled from the cloud.[135]

The Court therefore made explicit that accessing data stored beyond the phone would be an impermissible way to skirt the new rule.[136] Therefore, because *Riley*'s discussion encompasses GPS data stored remotely by a provider, and because locating a phone by its GPS

---

130. *See supra* note 18 and accompanying text.

131. Meyer, *supra* note 18; *see Sprint Locator*, *supra* note 34; *see, e.g.*, *State v. Subdiaz-Osorio*, 849 N.W.2d 748, 757 (Wis. 2014).

132. Although far from clear as to the precise mechanism, journalists report this type of law enforcement access has been going on since at least 2004. *See* Dana Priest, *NSA Growth Fueled by Need to Target Terrorists*, WASH. POST (July 21, 2013), http://wpo.st/v6Hi0. Moreover, at least at the federal level, law enforcement can access location data even when the phone is turned off. *See id.*

133. It bears repeating that a phone using A-GPS communicates with a cell provider's remote server—such communication in response to law enforcement requests clearly "accesses" data. *See* sources cited *supra* notes 18, 127.

134. *Cf. Subdiaz-Osorio*, 849 N.W.2d at 784 (Ziegler, J., concurring).

135. *Riley v. California*, 134 S. Ct. 2473, 2491 (2014).

136. *See id.*; Yip & Hsia, *supra* note 106, at 5 (concluding that the Court implied that an expectation of privacy attaches to information stored in the cloud). However, in a footnote the opinion made clear that it was not going to address the issue of the scope of the third-party doctrine with respect to remotely obtained data, *Riley,* 134 S. Ct. at 2489–90 n.1, discussed *infra* Part III.

involves accessing data stored both by the provider and directly on the phone,[137] the broad reading of *Riley* requires a warrant or exception before permitting a search.

There is one additional policy reason for the holding in *Riley* that could be used to support the narrow reading. One might argue that the holding in *Riley* was predicated on the notion of the "vast" amounts of data law enforcement might access if they were permitted to search a smart phone.[138] It follows that real-time GPS tracking potentially only involves the brief access of a miniscule amount of data, which in turn might not implicate the concerns that activated the Court.[139]

However, the Court addressed this as well, rejecting various solutions proposed by the government instead of a blanket warrant requirement.[140] The Court was therefore unmoved by solutions offered by the government that would limit searches to small amounts of data.[141] Similarly, it should not matter whether the amount of data searched in the real-time GPS tracking of a phone is relatively limited.[142]

---

137. *See supra* Part I.A.

138. *See* Shoebotham, *supra* note 67, at 40, 64; Barnes, *supra* note 84; *see also* Lamparello & MacLean, *supra* note 8, at 31–36.

139. *United States v. Bah*, 794 F.3d 617, 632 (6th Cir. 2015) (taking this approach in holding that the search of a magnetic strip on a suspect's credit card did not implicate the rule from *Riley* because of the miniscule storage capacity). *But cf. United States v. Jones*, 132 S. Ct. 945, 955 (2012) (Sotomayor, J., concurring) ("*GPS monitoring* generates a precise, comprehensive record of a person's public movements that *reflects a wealth of detail* about her familial, political, professional, religious, and sexual associations." (emphasis added)); Iqbal & Lim, *supra* note 3, at 45–46 (discussing the massive amounts of information GPS surveillance can reveal); *see also* Katie Shilton, *Four Billion Little Brothers?: Privacy, Mobile Phones, and Ubiquitous Data Collection*, COMM. ACM, Nov. 2009, at 39, 50–53.

140. Addressing the Government's proposed solutions, the Court stated:

> The United States also proposes a rule that would restrict the scope of a cell phone search to those areas of the phone where an officer reasonably believes that information relevant to the crime, the arrestee's identity, or officer safety will be discovered. This approach would again impose few meaningful constraints on officers. The proposed categories would sweep in a great deal of information, and officers would not always be able to discern in advance what information would be found where.
>
> We also reject the [proposal] that officers should always be able to search a phone's call log . . . .

Riley, 134 S. Ct. at 2492 (citation omitted); *see also* Margulies, *supra* note 16, at 42 (noting that Chief Justice Roberts rejected the development of law enforcement protocols because "the Founders did not fight a revolution to gain the right to government agency protocols" (quoting *Riley*, 134 S. Ct. at 2491)).

141. *See* Margulies, *supra* note 16, at 42; Weisselberg, *supra* note 84, at 165.

142. *Cf.* Lamparello & MacLean, *supra* note 8, at 35 (asserting that *Riley* did not address how the generalized privacy interest in cell data would apply to a less invasive search in terms of quantity).

III. LOWER COURT APPROACHES TO GPS TRACKING: IF *RILEY* "GENERALLY" REQUIRES A WARRANT WHAT ARE THE APPLICABLE EXCEPTIONS?

Whether one is persuaded that a decision limiting the search-incident-to-arrest doctrine naturally extends to GPS and other location-based tracking, it is clear that there is no agreement on this point among lower state and federal courts.[143] Although no exhaustive comparison has been made post-*Riley*, there is literature to suggest the trend may in fact be in favor of the narrow reading.[144] A full survey of all cell phone cases is beyond the scope of this Comment. Instead three cases—from Florida, the Fifth Circuit, and Wisconsin[145]—are compared to illustrate the approach applied by courts adopting a broader reading of *Riley*, as opposed to a narrow view. Additionally, the cases chosen provide a good framework for discussing which warrant exceptions should apply to GPS tracking and which should not.[146] By leaving the question open, *Riley* implicitly suggests that there is at least some limit as to which warrant exceptions get around the general rule.[147] This section discusses that limit.

---

143. *See supra* Part II.A. This disagreement—which includes both how broadly to read *Riley*, and what exceptions beyond exigent circumstances should apply to cell phone searches—underscores the need for both legislative standards and Supreme Court guidance.

144. *See* Curtis et al., *supra* note 18, at 80–89 (analyzing an emerging trend that in recent federal and state cases involving location-based tracking the state was far more likely to prevail at the suppression hearing).

145. *Tracey v. State*, 152 So. 3d 504 (Fla. 2014); *United States v. Guerrero*, 768 F.3d 351 (5th Cir. 2014); *State v. Subdiaz-Osorio*, 849 N.W.2d 748 (Wis. 2014).

146. *Riley*'s approval of exigencies resembles the approval given by the Court in *Payton* as to when a warrantless entry into the home is permissible. *Compare Riley v. California*, 134 S. Ct. 2473, 2494 (2014), *with Payton v. New York*, 445 U.S. 573, 590 (1979) ("Absent exigent circumstances, th[e] threshold [of the home] may not reasonably be crossed without a warrant."). *See also supra* note 8.

147. *See Riley*, 134 S. Ct. at 2494 (stating that other exceptions beyond exigent circumstances "may" apply to cell phone searches but declining to specify which). Possible exceptions that could apply to cell phone tracking are those that qualify as "exigent circumstances," those where government interests are heightened (e.g., border-search exception) and possibly those premised upon harmless error (e.g., the good-faith doctrine and inevitable-discovery rule). *See, e.g.*, *United States v. Stile*, No. 1:11-cr-00185-JAW, 2014 U.S. Dist. LEXIS 144241, at *17–22 (D. Me. Oct. 10, 2014) (applying inevitable discovery). *But see United States v. Camou*, 773 F.3d 932, 943–44 (9th Cir. 2014) (declining to apply inevitable discovery to the particular search at issue). *See also* Curtis et al., *supra* note 18, at 85–86; Lamparello & MacLean, *supra* note 8, at 35; *infra* Part III.D.

A. Florida: Reading Riley *and* Jones *Broadly to Require a Warrant*

The Supreme Court of Florida confronted warrantless GPS tracking of a cell phone in *Tracey v. State*.[148] The lower state courts concluded that *Karo* controlled the Fourth Amendment argument and had resolved the case under statutory tracking provisions.[149] Therefore, the precise issue before the State Supreme Court was "whether regardless of any . . . statutory provisions, the use of real time [cell-phone GPS] location information to track Tracey violated the Fourth Amendment . . . ."[150]

After discussion of the controlling Supreme Court precedent, the court concluded that no decision directly controlled the question.[151] The court therefore began its analysis by determining whether GPS tracking was a search in the first place under *Katz*.[152] In undertaking this analysis, the court used *Riley* in support of both prongs of that test.[153] Interestingly, the majority also noted that "nearly three-quarters of smart phone users report being within five feet of their phones most of the time,"[154] to demonstrate that GPS tracking is virtually certain to pierce into the home of a suspect.[155]

Another important piece of the analysis in *Tracey* was the court's conclusion that the third-party disclosure doctrine should be inapplicable to cell phone tracking.[156] According to several recent articles analyzing cases involving GPS tracking before and after *Riley*, one of the main ways courts resolve tracking cases is through the third-party doctrine.[157] As most of these cases do not implicate physical

148. 152 So. 3d 504 (Fla. 2014).

149. *Id.* at 508, 510.

150. *Id.* at 510–11. In distinguishing lower federal court precedent the court made clear that the issue in this case was "not *historical* cell site location information." *Id.* at 516 (emphasis added).

151. *Id.* at 512–15.

152. *Id.* at 512, 515.

153. *See id.* at 524–26.

154. *Id.* at 524 (quoting *Riley v. California*, 134 S. Ct. 2473, 2484 (2014)).

155. *See id.* Characterizing the intrusion as an entry to the home would result in a *per se* unreasonable search. *See Payton v. New York*, 445 U.S. 573, 589–90 (1979); *see also Kyllo v. United States*, 533 U.S. 27, 40 (2001) (concluding that thermal imaging of a home was a search because it penetrated the walls of the home and revealed details not known to the public).

156. *See Tracey*, 152 So. 3d at 523. *But cf. id.* at 526 n.17 (Canady, J., dissenting) (holding open the possibility of other bases for exception to the warrant requirement); *id.* at 526–29 (Canady, J., dissenting) (concluding that cell site location information is subject to the third-party disclosure doctrine).

157. Wackman, *supra* note 6, at 301; *see also* Curtis et al., *supra* note 18, at 86–87.

trespass and instead involve tracking over extended periods,[158] one way to avoid the concerns discussed by Justice Alito's concurrence in *Jones*,[159] is for courts to conclude that the use of one's cell phone entails a voluntary disclosure to a third party.[160] The Florida Supreme Court found this conclusion unconvincing, which is significant given the number of pre-*Riley* cases to the contrary.[161]

B. Fifth Circuit: Reading Riley *as Strictly Limited to Search Incident to Arrest*

In *United States v. Guerrero*,[162] the Fifth Circuit confronted the issue of improperly obtained historic cell site data and GPS tracking.[163] The court concluded that the search did not meet the requirements of the Stored Communications Act,[164] but resolved the case under circuit precedent after concluding that *Riley* had not overruled its precedent with respect to location data under the third-party doctrine.[165] Although the case dealt primarily with historic cell site data as opposed to GPS,[166] the court's discussion of *Riley* is particularly useful to the argument that the third-party doctrine should not apply in the latter situation.[167]

---

158. *See* Curtis et al., *supra* note 18, at 83–84, 88–90.

159. *United States v. Jones*, 132 S. Ct. 945, 962–64 (2012) (Alito, J., concurring).

160. *See* Curtis et al., *supra* note 18, at 86–87; *see, e.g.*, *United States v. Guerrero*, 768 F.3d 351, 359–61 (5th Cir. 2014). Professor Orin Kerr has contended that no decisions from the Court require the recognition of a Fourth Amendment privacy interest in records voluntarily disclosed to a third party. Orin Kerr, *DOJ Petitions for Rehearing in Eleventh Circuit Cell-Site Case*, WASH. POST (Aug. 1, 2014), http://www.washingtonpost.com/news/volokh-conspiracy/wp/2014/08/01/doj-petitions-for-rehearing-in-eleventh-circuit-cell-site-case. However, other commentary disagrees with this, at least with respect to location-based tracking. *See* Pincus, *supra* note 2, at 333–34.

161. *See Tracey*, 152 So. 3d at 525; Curtis et al., *supra* note 18, at 86, 92–100 (listing pre-*Riley* cases).

162. 768 F.3d 351 (5th Cir. 2014).

163. *Id.* at 357–58.

164. *Id.* at 358; *see* 18 U.S.C. § 2703(d) (2012) (delineating requirements for obtaining certain kinds of stored, aggregate information).

165. *Guerrero*, 768 F.3d at 359–61. The Fifth Circuit emphasized the portions of *Riley* that typically are used to favor a narrow reading, namely: (1) that the Court's statement of the issues was confined to search incident to arrest; and (2) that the Court distinguished *Smith v. Maryland*, 442 U.S. 735 (1979) (third-party doctrine), by emphasizing that in *Riley* there was no dispute that a search had occurred. *Guerrero*, 768 F.3d at 359–60 (citing *Riley v. California*, 134 S. Ct. 2473, 2489 n.1 (2014)).

166. For an explanation of the distinction, see *supra* note 18.

167. *But see* Barry Friedman, *in How the Supreme Court Changed America This Year*, POLITICO MAG. (July 1, 2014), http://www.politico.com/magazine/story/2014/07/how-the-supreme-court-changed-america-this-year-108497 ("Those who

The court's conclusion that *Riley* had not changed the third-party doctrine with respect to location information is suspect for two reasons. First, the portion of *Riley* that distinguished *Smith v. Maryland*[168] stated, "call logs typically contain more than just phone numbers; they include any identifying information that an individual might add, such as the label 'my house' . . . ."[169] If the Supreme Court found the adding of labels to phone numbers to be enough of a distinction to take *Riley* outside of the third-party doctrine, then it would seem that precise location information should have the same distinguishing effect.[170] And second, the issues in real-time GPS tracking reach directly into the data within the phone. Causing a phone to broadcast its location tortures the logic of the exception—which is based on the voluntary exchange of information by the defendant with a third party.[171]

C. Wisconsin: No Consensus on the Role of Riley

In *State v. Subdiaz-Osorio*,[172] the Supreme Court of Wisconsin determined that the warrantless real-time tracking of a suspect did not violate the Fourth Amendment.[173] The fractured decision produced six opinions out of the seven justices.[174] The differing rationales illustrate the need for clarity within the tracking doctrine.

Justice Prosser's lead opinion resolved the tracking issue by assuming a search,[175] but concluding that the exigent circumstances of the defendant fleeing the country and probable cause for a warrant created an exception to the requirement.[176] Justice Crooks concurred in the result but extensively discussed the applicability of *Riley*.[177] His

---

believe the justices will leap from *Riley* to overturning the third party doctrine are dreaming.").

168. 442 U.S. 735 (1979).

169. *Riley*, 134 S. Ct. at 2493. In *Smith*, the Court held that no search occurred when law enforcement used a pen register device, which recorded only numbers dialed. *Smith*, 442 U.S. at 745–46. The information was "voluntarily" given to the phone company. *Id.* at 746. Though not explicitly creating anything called the "third-party doctrine," the case is frequently cited for that proposition. *See, e.g.*, *Rehberg v. Paulk*, 611 F.3d 828, 843 (11th Cir. 2010).

170. *But cf.* Friedman, *supra* note 167.

171. *See In re Application of the U.S. for an Order Directing a Provider of Elec. Commc'n Serv. to Disclose Records to the Gov't*, 620 F.3d 304, 317–18 (3d Cir. 2010) (distinguishing *Smith* on precisely this ground).

172. 849 N.W.2d 748 (Wis. 2014).

173. *Id.* at 752.

174. *See id.* at 752 & n.3.

175. *Id.* at 752. Three of the justices went further than this assumption and would have held that a search occurred. *See id.* at 752 n.3.

176. *Id.* at 752 n.4.

177. *See id.* at 776–77 (Crooks, J., concurring).

concurring opinion stated that the "holding[] of the . . . Supreme Court in [*Riley*] . . . lead[s] me to the conclusion that, absent case-specific exceptions, such as an emergency, a warrant is required for the search of a cell phone's location."[178] Nevertheless, Justice Crooks concurred in the result applying a good-faith exception.[179] In contrast, Justice Bradley would have resolved the case under harmless error,[180] while Justice Roggensack would have avoided discussion of the privacy implications of GPS tracking, deciding that issue solely on the basis of the exigent circumstances.[181] Significantly, all of the justices who discussed the third-party doctrine questioned whether it needed to be re-evaluated in light of the privacy implications recognized by *Riley*.[182]

D. Exigencies and Reduced Expectations of Privacy: Which Warrant Exceptions Should Apply?

Several observations emerge from the discussion of these examples. First, courts are struggling with how to apply *Riley* beyond search incident to arrest.[183] The broad privacy language regarding cell phones appears especially difficult for courts to reconcile,[184] given the intrusive nature of GPS tracking. Second, courts vary in the applicability of *Riley* to GPS tracking versus historical cell site location information. And third, courts appear to have incorporated virtually every warrant exception into the requirement.[185]

With respect to the third observation, it is clear that *Riley* did not intend to preclude the application of warrant exceptions to cell phone searches. The Court explicitly adopted exigent circumstances and left the question open as to other exceptions.[186] However, the Court also did

178. *Id.* (Crooks, J., concurring); *but see id.* at 784 (Ziegler, J., concurring) (declining to determine whether the location of a cell phone as opposed to the contents contained were subject to the same constitutional analysis under *Riley*).

179. *Id.* at 776–77 (Crooks, J., concurring).

180. *Id.* at 773 (Bradley, J., concurring).

181. *Id.* at 782 (Roggensack, J., concurring). The chief justice dissented on the grounds that a search occurred and any resulting error was not harmless. *Id.* at 786 (Abrahamson, C.J., dissenting).

182. *See id.* at 789 (Abrahamson, C.J., dissenting); *cf. id.* at 783 (Roggensack, J., concurring); *see also State v. Tate*, 357 Wis. 2d 172, 849 N.W.2d 798, 805 & n.11 (Wis. 2014).

183. *See supra* Part III.A–C.

184. *Compare Subdiaz-Osorio*, 849 N.W.2d at 776 (Crooks, J., concurring), *with id.* at 784 (Ziegler, J., concurring).

185. *See State v. Henderson*, 854 N.W.2d 616, 635 (Neb. 2014) (holding a cell phone warrant to be invalid but applying the good-faith exception); *see generally* cases cited *supra* Part II.A.

186. *Riley v. California*, 134 S. Ct. 2473, 2494 (2014).

not endorse a wholesale application of all warrant exceptions and implied that there was *some* limiting principle.[187]

In light of this, this Part closes with the following recommendation as to how courts should analyze whether to incorporate a given exception. Reviewing courts should begin by recognizing the privacy interests attached to cell phones as stated in *Riley*.[188] Using that rationale as a guide, courts should proceed with the analysis as to whether an exception applies in the same manner that the Court did in *Riley*. Specifically, within a given exception the inquiry should be whether the rationale for a given exception is undercut by the "qualitative" and "quantitative" differences between cell phones and other articles.[189]

An example is useful to illustrate this proposed analysis. In determining whether to incorporate the third-party doctrine, the court would begin by examining the reasoning for the exception. The third-party doctrine is premised on the rationale of voluntarily disclosed information, given for some benefit.[190] That rationale is inapplicable to GPS tracking, best illustrated by the Third Circuit's statement that a "cell phone customer has not 'voluntarily' shared his location information with a cellular provider in any meaningful way."[191] Moreover, the privacy concerns attached to permitting searches based on the "exception"[192] are in no way lessened or different from those discussed in *Riley*. Therefore, in light of the privacy implications and the fact that the "voluntariness" of exchanging data from an always-active GPS system is markedly different from the telephone numbers in *Smith*,[193] a court should reject applying the exception in the cell phone context.[194]

---

187. *See id.* ("[o]ther . . . exceptions *may* [apply] . . . ." (emphasis added)); *id.* at 2492–93 (declining to address the government's arguments regarding the third-party doctrine as a search was conceded).

188. *Id.* at 2488.

189. *Id.* at 2489.

190. *See Smith v. Maryland*, 442 U.S. 735, 743–44 (1979). It is worth noting that the "third-party doctrine" is not really an exception to the warrant requirement, but rather a *per se* "no search" rule. In deciding *Smith*, the Court concluded that there was no reasonable expectation of privacy in voluntarily disclosed records—i.e., the *Katz* test was *per se not* met. *See id.* If *Riley* stands for the proposition that *Katz* is satisfied whenever cellular data is accessed, then *Smith*'s no-search rule should be irrelevant (at least from a formalist perspective).

191. *See In re Application of the U.S. for an Order Directing a Provider of Elec. Commc'n Serv. to Disclose Records to the Gov't*, 620 F.3d 304, 317 (3d Cir. 2010).

192. Again, the doctrine is not really an exception. *See supra* note 190.

193. Unlike the telephone records in *Smith*, a phone's GPS is always on, or at least always capable of being switched on by a provider. The *Smith* court reasoned that an individual was sharing phone numbers with a provider in exchange for the benefit of

The Sixth Circuit seemingly applied this approach to the "private search warrant exception," which requires law enforcement to stay within a virtual certainty of the scope of a prior search done by a private individual.[195] In *United States v. Lichtenberger*,[196] law enforcement searched the defendant's laptop without a warrant after his girlfriend reported that it contained child pornography.[197] In holding that the exception did not apply to the search, the court first extended *Riley*'s digital-content rule to laptops.[198] But more importantly, the court analyzed the justifications for the private-search exception and found them dramatically wanting compared to the enormous privacy interests at stake when law enforcement are able to search the entirety of a computer's contents.[199]

CONCLUSION

The Court in *Riley* created a rule requiring a warrant before searching data contained on a cell phone. That rule should be read broadly, extending beyond the search-incident-to-arrest exception. Reading the rule narrowly ignores the plain language of the decision and frustrates the underlying policy articulated by the Court,[200] essentially reducing its protection to prohibiting the government from examining recent calls or messages at the scene of an arrest.[201]

Additionally, reviewing courts should not skirt the rule by a wholesale incorporation of all warrant exceptions. Instead, courts should carefully scrutinize whether the reasons for a given exception hold up against the privacy interests of cell phones. This inquiry is exactly what

---

calling. *See Smith*, 442 U.S. at 742. But again, unlike GPS, a phone is not always calling, and a provider cannot force a phone to call certain numbers in response to a request from police.

194. *See* Adam Lamparello & Charles MacLean, Riley v. California*: The New* Katz *or* Chimel*?*, 21 RICH. J.L. & TECH. 1, 16–17 (2014) (positing that the problems the Court saw with applying search incident to arrest to cell phones are identical to those in applying the third-party doctrine). *But see* Wackman, *supra* note 6, at 296–99, 313 (defending the doctrine's utility as to historical cell data).

195. *United States v. Lichtenberger*, 786 F.3d 478, 485–91 (6th Cir. 2015).

196. 786 F.3d 478 (6th Cir. 2015).

197. *Id.* at 479–81. Lichtenberger's girlfriend had discovered the illicit material after she "hacked into Lichtenberger's personal laptop computer . . . ." *Id.* at 479.

198. *See id.* at 488.

199. *See id.* at 490–91.

200. While the broader reading could be said to suffer from the same flaw, such a reading is in harmony with the Court's discussion of the privacy concerns attendant to searches of cell data.

201. *See* Lamparello & MacLean, *supra* note 8, at 32–35; *see, e.g.*, *Commonwealth v. Sheridan*, 25 N.E.3d 875, 884–85 (Mass. 2015) (suppressing text messages searched incident to arrest).

the Court did in *Riley* and is in line with the Court's approach in other cases implicating new technologies[202]—favoring evaluating intrusions against justifications rather than blindly applying a rule.[203]

Unfortunately, it appears that the majority of courts confronting cell phone searches are taking the narrow reading of the decision and limiting it to the search-incident-to-arrest context.[204] As is often the case when a decision from the Court upsets a widespread police practice,[205] the issue is being frequently litigated—and the willingness of courts to apply *Riley* to GPS tracking is still unclear. What is clear however is that no consensus has emerged as to either the applicability of *Riley* or the exceptions that should apply.[206]

Looking forward, the Court should take another opportunity to clarify the conflicts that remain among the lower courts. In the interim, Congress and state legislatures should take up the issue.[207] But while legislative efforts are important, they do not obviate the need to clear up the constitutional questions. As a matter of constitutional law, is GPS tracking beyond the scope of the rule articulated in *Riley*? Or has the Court elevated cell phones within the category of the home? To paraphrase the English adage: is a person's cell phone now his or her castle?

---

202. *See, e.g.*, *Kyllo v. United States*, 533 U.S. 27 (2001).

203. *See* Lamparello & MacLean, *supra* note 8, at 40; Ricciuti & Parker, *supra* note 6, at 9.

204. *See* cases cited *supra* notes 72–77; *see generally* Curtis et al., *supra* note 18.

205. *See, e.g.*, *Arizona v. Gant*, 556 U.S. 332, 343 (2009).

206. *See supra* Part III.A–C; cases cited *supra* Part II.A.

207. *See* Wackman, *supra* note 6, at 314–18 (proposing a variety of recommendations to deal with the retention of historic cell site information). Wackman specifically recommends the creation of a Suppression Remedy in the Federal Stored Communications Act. *Id.* at 314–15; *see* 18 U.S.C. §§ 2701–12 (2012). Additionally, the Senate recently held hearings over a bill that would require a warrant before law enforcement could engage in any kind of GPS tracking, including cell phones. *See* Hattem, *supra* note 22. And in Wisconsin, Governor Walker recently signed a GPS tracking statute specifying in detail the procedure police must follow to track a cell phone, as well as to what extent cellular providers may be held liable for disclosures. *See* WIS. STAT. §§ 968.373(2)–(8), 968.375(11), (13) (2013–14).