Fordham Law Review

Volume 81 | Issue 1 Article 9

2012

Track Me Maybe: The Fourth Amendment and the Use of Cell Phone Tracking to Facilitate Arrest

Jeremy H. Rothstein
Fordham University School of Law

TRACK ME MAYBE: THE FOURTH AMENDMENT AND THE USE OF CELL PHONE TRACKING TO FACILITATE ARREST

*Jeremy H. Rothstein**

Police use of technology to locate and track criminal suspects has drawn increasing attention from courts, commentators, and the public. In United States v. Jones*, the Supreme Court held that police installation of a GPS tracking device on a suspect's vehicle constituted a search under the Fourth Amendment. Less attention has been paid to police tracking of cell phones—a far more common practice. Police can now locate a cell phone within several feet, using either GPS or information taken from cell towers.*

In August 2011, the government asked a federal magistrate judge in Maryland to allow thirty days of cell phone GPS tracking to aid in the apprehension of the subject of an arrest warrant. The judge denied the application, ruling that precise tracking for any period would be a search, and that an arrest warrant did not make the search reasonable under Payton v. New York*, which allows officers to arrest the subject of an arrest warrant in his home if the officers reasonably believe he is present.*

This Note examines the magistrate judge's opinion, considers critical commentary, and analyzes a 2006 district court case holding that imprecise tracking to aid apprehension was constitutional. Cell phone tracking raises different issues than the vehicular GPS considered in Jones*. Cell phone tracking does not involve a physical trespass, but it does follow individuals into private spaces. The Note concludes that precise cell phone tracking is a search and argues that such a search could be reasonable under* Payton*, but only if carefully limited. While cell phone tracking to aid arrest increases public safety by helping police arrest criminal suspects quickly and efficiently, it should not be used to find evidence of crime. Judges should only allow tracking for one or two days to ensure that police quickly apprehend subjects of arrest warrants, rather than exploit cell phones to conduct unauthorized investigations.*

TABLE OF CONTENTS

* J.D. Candidate, 2013, Fordham University School of Law. Thanks go to my faculty advisor Martha Rayner. Also to Margaret Wheeler, my fiancée Kali Peterson, and my parents Claire Herzberg and Alan Rothstein.

INTRODUCTION

Police track thousands of cell phones every year.[1] Generally, neither the target nor the public ever learns of a tracking order.[2] Requests to track cell phones are sealed, and the judges who consider them seldom publish opinions.[3] One federal magistrate judge has estimated that federal courts alone approve 20,000–30,000 tracking requests annually, and the number is rising.[4] This Note examines the constitutionality of tracking a cell phone belonging to the subject of an arrest warrant to facilitate his arrest.

There is no consensus as to whether cell phone tracking constitutes a search under the Fourth Amendment.[5] In only the past few years, technological advances have enabled cell phone tracking to provide an accurate location to within several feet.[6] The pace of change has rendered obsolete court decisions from even four years ago: cases that considered technology that could only place users within hundreds of feet.[7] While the

1. Julia Angwin & Scott Thurm, *Judges Weigh Phone Tracking*, WALL ST. J., Nov. 9, 2011, at A1.

2. *Id.*

3. *Id.* ("Little is known about the practice because tracking requests are typically sealed from public view.").

4. *Id.* ("Magistrate Stephen Smith of Houston, Texas, who approves such surveillance orders, has been studying the available data and estimates that federal courts alone issue 20,000 to 30,000 cellphone tracking orders annually.").

5. *Id.* ("The widening practice also presents one of the biggest privacy questions in a generation . . . .").

6. *See infra* Part I.A.

7. *See infra* Part I.B.4.c.

issue is by no means closed, no published opinions have approved the use of precise cell phone tracking in a criminal investigation without a search warrant,[8] and the only district court judge to rule on the issue found it unconstitutional.[9] But criminal investigations are not the only law enforcement use for cell phone tracking.

In August 2011, police asked Magistrate Judge Susan K. Gauvey of the District of Maryland to authorize precise, persistent cell phone tracking to locate the subject of an arrest warrant.[10] The government argued that cell phone tracking is not a search and that, even if tracking is a search, *Payton v. New York*,[11] which allows officers to enter a private home for the limited purpose of executing an arrest warrant, permits the "lesser intrusion" of cell phone tracking.[12] Judge Gauvey disagreed and issued an extensive opinion, *In re United States for an Order Authorizing Disclosure of Location Information of a Specified Wireless Telephone*[13] (*Specified Wireless Telephone*), finding that precise, persistent cell phone tracking to facilitate arrest was unconstitutional.[14] The decision drew criticism from Professor Orin Kerr, who argued that such tracking is constitutional. This Note examines both perspectives.[15]

Determining the constitutionality of precisely tracking a cell phone to facilitate arrest involves two distinct questions: First, is precise, persistent cell phone tracking a search within the meaning of the Fourth Amendment? And second, if cell phone tracking does constitute a search, would that search be reasonable if used to aid in the apprehension of the subject of an arrest warrant? To answer these questions, this Note also analyzes *United States v. Bermudez*,[16] a 2006 district court case that held that *Payton* justified brief, imprecise tracking.[17]

Part I outlines the technologies and constitutional doctrines at issue. Then, Part II explores the controversy over cell phone tracking with an arrest warrant. Finally, Part III argues that while cell phone tracking constitutes a search under the Fourth Amendment, it can be a reasonable one. Under court supervision, limited use of cell phone tracking to apprehend the subject of an arrest warrant is constitutional.

---

8. *See infra* Part I.B.4.c.

9. *In re* U.S. for Historical Cell Site Data, No. 11-MC-223 (S.D. Tex, Nov. 11, 2011), *available at* http://online.wsj.com/public/resources/documents/hughesorder1116.pdf.

10. *In re* U.S. for an Order Authorizing Disclosure of Location Info. of a Specified Wireless Tel., No. 10-2188-SKG, 2011 WL 3423370 (D. Md. Aug. 3, 2011) [hereinafter *Specified Wireless Tel.*].

11. 445 U.S. 573 (1980).

12. *See infra* notes 325–26 and accompanying text.

13. 10-2188-SKG, 2011 WL 3423370 (D. Md. Aug. 3, 2011).

14. *See infra* Part II.A.

15. *See* Part II.B.2.

16. No. IP 05-43-CR-B/F, 2006 WL 3197181 (S.D. Ind. June 30, 2006), *aff'd on other grounds sub nom.* United States v. Amaral-Estrada, 509 F.3d 820, 829 (7th Cir. 2007). On appeal the Seventh Circuit did not review the cell phone tracking issue. Amaral-Estrada, 509 F.3d at 829.

17. *Bermudez*, 2006 WL 3197181, at *11.

I. ELECTRONIC LOCATION TRACKING AND THE FOURTH AMENDMENT

The Fourth Amendment protects Americans from unreasonable searches and seizures.[18] To determine the constitutionality of precise, persistent tracking to facilitate arrest, a court must first decide whether the practice is a search. If it is, the court must then consider whether the arrest warrant makes that search reasonable. Part I.A examines the technology police use to track cell phones. Part I.B analyzes the doctrines courts apply to determine whether a police practice is a search and discusses the application of those doctrines to new technology. Part I.C explains the requirements of arrest and search warrants, and considers the power of an arrest warrant under *Payton*.

A. Cell Phone Tracking and Its Use by Law Enforcement

In a very short time, consumer location technology has become ubiquitous. It has also become increasingly accurate. This section details the evolution and future of the two technologies used to track phones: the Global Positioning System (GPS) and cell-site location information. It then provides a brief overview of the use of this technology by police.

1. GPS

GPS is a constellation of satellites operated by the U.S. Air Force.[19] A device communicating with the GPS satellites can calculate its own velocity and location in three dimensions.[20] All phones sold since 2003 are GPS-enabled.[21] GPS technology in cell phones can typically calculate location to within ten meters[22] and will become more accurate in the near future.[23] However, tracking with GPS technology has certain limitations. Whether a phone transmits GPS data depends on the network and on the phone's applications that use GPS.[24] A user can disable her phone's GPS, and because GPS currently requires a "view" of the satellites, it can be unreliable indoors.[25]

---

18. U.S. CONST. amend. IV.

19. *Global Positioning System Factsheet*, U.S. AIR FORCE (Sept. 15, 2010), http://www.af.mil/information/factsheets/factsheet.asp?id=119.

20. *Id.*

21. The FCC requires all phones to be GPS-enabled to facilitate emergency location under Enhanced 911 Phase II. *See Enhanced 911*, VERIZON WIRELESS, http://aboutus.verizonwireless.com/wirelessissues/enhanced911.html (last visited Sept. 21, 2012).

22. *ECPA Reform and the Revolution in Location Based Technologies and Services: Hearing Before the Subcomm. on the Constitution, Civil Rights, and Civil Liberties of the H. Comm. on the Judiciary*, 111th Cong. 14 (2010) [hereinafter *Blaze Testimony*], *available at* http://judiciary.house.gov/hearings/printers/111th/111-109_57082.PDF (statement of Matt Blaze, Professor, University of Pennsylvania).

23. Potential near-future developments include GPS III satellites capable of three times the accuracy. Press Release, Lockheed Martin, Lockheed Martin Team Completes Design Milestone for GPS III Program (July 5, 2011), *available at* http://www.lockheedmartin.com/us/news/press-releases/2011/july/gps3-sdr.html.

24. *Blaze Testimony*, *supra* note 22, at 22. Some applications will use GPS information to search for nearby restaurants, for instance. *Id.* at 21–22.

25. *Id.* at 22.

2. Cell-Site Location Information

Phones can also be tracked using cell-site location information (CSLI). Cellular service providers have a network of base stations (cell phone towers) spread throughout their coverage area.[26] Any phone with service will be within range of at least one tower.[27] Most users will be within range of multiple base stations and, in urban areas, they can be so densely packed that one base station may only cover a building or just an individual floor.[28] By calculating the time and angle at which cell phone signals reach three towers (a process called triangulation), service providers can track cell phone location to within fifty meters.[29] As technology becomes more accurate,[30] the distinction between "high accuracy" GPS and "low accuracy" CSLI will be effectively eliminated.[31]

CSLI requires no special device capability, cannot be disabled by the user, and is collected and analyzed at the providers' base stations rather than on the device itself.[32] All providers record this location information when a phone sends and receives text messages and at the beginning and end of each call, but many providers also periodically collect it for various business purposes without any action by the user.[33]

3. Cell Phone Tracking By Law Enforcement

Law enforcement officers primarily use three types of cell phone tracking information: historical CSLI, real-time CSLI, and GPS. In a request for historical CSLI, the government will ask the court to order a service provider to turn over the records of a consumer's location recorded in the ordinary course of business.[34] The information in these records is increasingly precise, and it is recorded frequently.[35] Officers can also acquire a court order to obtain prospective CSLI in real-time or upon request, which allows for minute-to-minute tracking.[36] New technology

---

26. *Id.* at 23.
27. *Id.*
28. *Id.* at 25.
29. *See id.* at 26.
30. *Id.* at 29. ("For a typical user, over that time, [CSLI] will likely have a locational precision similar to that of GPS.")
31. *In re* U.S. for Historical Cell Site Data, 747 F. Supp. 2d 827, 834 (S.D. Tex. 2010) [hereinafter *Judge Smith Op.*].
32. *See Blaze Testimony*, *supra* note 22, at 22.
33. *See id.* at 27. Providers are collecting information for two reasons: (1) in response to Congressional and FCC directives to enhance the Emergency 911 system, and (2) to help determine where improvements to their infrastructure are needed. *See Judge Smith Op.*, 747 F. Supp. 2d at 833; *Blaze Testimony*, *supra* note 22, at 27. Cell phones register or "handshake" with towers approximately eight times a minute, and each "handshake" can be recorded. David H. Goetz, Note, *Locating Location Privacy*, 26 BERKELEY TECH. L.J. 823, 837 (2011).
34. *See Judge Smith Op.*, 747 F. Supp. 2d at 829–30. Data can include not just the sector, but the phone's latitude and longitude. A record of texts and calls would provide twenty to fifty-five location points a day. *Id.* at 835.
35. *Id.* at 833.
36. *Id.* 835–36.

allows the police to obtain CSLI on their own, without compelling service providers.[37] These mobile "stingray" devices can mimic cell phone towers and ping[38] a phone to reveal its location.[39]

For GPS, the court will order a provider to ping a phone at times or intervals specified by the officers.[40] The ping directs the device to calculate its location and send it to the provider, which forwards it to the officers.[41] Orders authorizing tracking are usually accompanied by a gag order preventing the service provider from notifying consumers that the government is accessing their location information.[42] Because the records are routinely placed under indefinite seal, neither the target nor the public knows of the surveillance.[43]

This Note will group the above technologies into two categories. The first is precise, persistent tracking, which allows the police to determine, at small intervals, the subject's exact location to within a few meters or less. Both GPS and CSLI are now capable of such tracking. The second category is imprecise, intermittent tracking, which allows the police to determine the subject's location within several hundred meters. It only documents the subject's position when he calls or texts. The law surrounding each of these uses will be discussed in Part I.B.4.c.[44]

B. Fourth Amendment Protection Against Unreasonable Searches

The Fourth Amendment provides:

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.[45]

---

37. Jennifer Valentino-DeVries, *"Stingray" Phone Tracker Fuels Constitutional Clash*, WALL ST. J., Sept. 22, 2011, at A1.

38. A "ping" is a signal sent to a device that causes it to respond. *Id.*

39. *Id.* These devices are called "stingrays" or "triggerfish." *Id.* The law on these devices is murky. *See id. See generally* William Curtiss, Note, *Triggering A Closer Review: Direct Acquisition of Cell Site Location Tracking Information and the Argument for Consistency Across Statutory Regimes*, 45 COLUM. J.L. & SOC. PROBS. 139 (2011) (examining "the unique legal and practical implications of the use of triggerfish" and arguing that their use should require a showing of probable cause).

40. *Specified Wireless Tel.*, No. 10-2188-SKG, 2011 WL 3423370, at *2 (D. Md. Aug. 3, 2011).

41. *Id.* at *1.

42. *ECPA Reform and the Revolution in Location Based Technologies and Services: Hearing Before the Subcomm. on the Constitution, Civil Rights, and Civil Liberties of the H. Comm. on the Judiciary*, 111th Cong. 80 (2010) [hereinafter Smith Testimony], *available at* http://judiciary.house.gov/hearings/printers/111th/111-109_57082.PDF (statement of Stephen Wm. Smith, U.S. Mag. J.).

43. *Id.*

44. Many of the cases discussed involve imprecise, intermittent tracking, but this Note only evaluates precise, persistent tracking to facilitate arrest.

45. U.S. CONST. amend. IV.

The first clause protects against unreasonable searches and seizures conducted without a warrant.[46] The second regulates warrants, requiring that they be based on probable cause and supported by a sworn affidavit.[47] Warrants must also describe with particularity both the place to be searched and the persons or things to be seized.[48] For a police practice to violate the first clause, it must be a search and that search must be unreasonable.[49] This section explores developments in Fourth Amendment jurisprudence as it adapts to new surveillance technology.

1. The History of Restrictions on Unreasonable Searches

The primary aim of the Fourth Amendment was to eliminate the colonial "general warrant,"[50] which gave customs officials broad authority to search for contraband anywhere, including private homes.[51] Until the 1960s, property rights largely determined the reasonableness of a search: if the government trespassed on property, then the search was unreasonable.[52] The protection extended as much to private papers as to the home, but was limited to areas and objects in which a person had a property interest.[53]

2. *Katz* and the Reasonable Expectation of Privacy

In *Katz v. United States*,[54] the Supreme Court rejected the exclusively property-based conception of the Fourth Amendment, ruling that it "protects people, not places."[55] In his concurrence, Justice Harlan formulated a two-prong test to determine constitutional protection[56] that became the standard analysis in subsequent cases applying *Katz*.[57] Under Justice Harlan's test, a person must (1) have "exhibited an actual (subjective) expectation of privacy," and (2) society must be prepared to

46. Payton v. New York, 445 U.S. 573, 585 (1980).

47. Groh v. Ramirez, 540 U.S. 551, 557 (2004).

48. *Id.* An arrest is the seizure of a person. *See, e.g.*, Terry v. Ohio, 392 U.S. 1, 10 (1968).

49. *See Terry*, 392 U.S. at 9.

50. *See* Stanford v. Texas, 379 U.S. 476, 481 (1965).

51. *See id.* Not just an instrument of colonial oppression, general warrants had been used in Britain since the Tudors, until they were condemned by British courts and the House of Commons in the 1760s. *See* Boyd v. United States, 116 U.S. 616, 625–26 (1886).

52. *See* United States v. Jones, 132 S. Ct. 945, 949 (2012) ("[O]ur Fourth Amendment jurisprudence was tied to common-law trespass, at least until the latter half of the 20th century."); *Boyd*, 116 U.S. at 630. In British and American common law, "every invasion of private property, be it ever so minute, is a trespass." *Id.* at 627.

53. *See* Richard G. Wilkins, *Defining the "Reasonable Expectation of Privacy": An Emerging Tripartite Analysis*, 40 VAND. L. REV. 1077, 1084 (1987).

54. 389 U.S. 347 (1967).

55. *Id.* at 351. As the Court explained in *Jones*, *Katz* expanded Fourth Amendment protection—it did not replace the property-based test. *Jones*, 132 S. Ct. at 950–51 (citing Alderman v. United States, 394 U.S. 165, 180 (1969) ("Nor do we believe that *Katz*, by holding that the Fourth Amendment protects persons and their private conversations, was intended to withdraw any of the protection which the Amendment extends to the home.")).

56. *Katz*, 389 U.S. at 361 (Harlan, J., concurring).

57. *See* Thomas K. Clancy, *What Is a "Search" Within the Meaning of the Fourth Amendment?*, 70 ALB. L. REV. 1, 54 n.121 (2006).

recognize that expectation as reasonable.[58] Recent decisions, however, often subordinate the first prong or ignore it outright.[59]

3. What Expectations Are Reasonable?

Court determinations of what constitutes a reasonable expectation of privacy are notoriously unpredictable.[60] Orin Kerr's article, *Four Models of Fourth Amendment Protection*,[61] is a helpful guide through this jungle. Kerr breaks Supreme Court decisions into four "distinct but coexisting approaches."[62] These models each consider different factors because, Kerr observes, no single test can accurately determine which police practices are reasonable on every set of facts.[63]

The four models he suggests are the probabilistic model, the private facts model, the positive law model, and the policy model.[64] The probabilistic model assesses the likelihood that a person or place would be observed.[65] A person has a reasonable expectation of privacy when the odds are high that "others will not successfully pry into his affairs."[66] For example, squeezing soft luggage to search for narcotics is a search, because a person does not expect his bag to be handled in an exploratory manner.[67]

The private facts model considers the information that the government collects rather than the methods used to procure it.[68] Even though people have an expectation of privacy in their mail, a chemical field test for narcotics is not a search, because it reveals nothing more than whether a package contains narcotics.[69] The private facts model is often applied to cases involving new technologies.[70]

---

58. *See Katz*, 389 U.S. at 361 (Harlan, J., concurring).

59. *See* WAYNE R. LAFAVE, 1 SEARCH & SEIZURE § 2.1(c) (4th ed. 2011) ("[L]ittle attention has been given to the independent significance of the first factor or to precisely how it is to be interpreted."); Renée McDonald Hutchins, *The Anatomy of a Search: Intrusiveness and the Fourth Amendment*, 44 U. RICH. L. REV. 1185, 1191 (2010) ("Increasingly, significant analysis of the first prong of the *Katz* test is noticeably absent from the Court's search jurisprudence.").

60. 1 LAFAVE, *supra* note 59, § 2.1(b) ("[I]t can hardly be said that the Court produced clarity where theretofore there had been uncertainty."); Anthony G. Amsterdam, *Perspectives on the Fourth Amendment*, 58 MINN. L. REV. 349, 349 (1974) ("For clarity and consistency, the law of the fourth amendment is not the Supreme Court's most successful product.").

61. Orin S. Kerr, *Four Models of Fourth Amendment Protection*, 60 STAN. L. REV. 503 (2007).

62. *See id.* at 506.

63. *Id.* at 525.

64. *Id.* at 506.

65. *See id.* at 508.

66. *See id.* 508–09.

67. *See id.* at 509 (citing Bond v. United States, 529 U.S. 334, 339 (2000)).

68. *See* Kerr, *supra* note 61, at 512–13.

69. *See id.* at 513 (citing United States v. Jacobsen, 466 U.S. 109, 123 (1984)); *see also* United States v. Place, 462 U.S. 696, 707 (1983) (holding constitutional the use of drug sniffing dogs on luggage).

70. *See* Kerr, *supra* note 61, at 543.

The positive law model asks if the government violated some law to obtain information.[71] This inquiry often resembles pre-*Katz* property-based Fourth Amendment analysis, but the Court does apply it in other contexts.[72] For instance, the government is permitted to fly a helicopter at low altitude over a defendant's house if flying at such altitudes is legal for private citizens.[73]

The policy model weighs the cost to civil liberties against the consequences of restricting police investigative power.[74] While the policy model is often invoked explicitly, Kerr suggests that it also implicitly guides many decisions that apply the other models.[75] Policy model cases employ overtly normative arguments.[76] For example, in holding that pointing a thermal imaging device at a house to detect marijuana plants was unconstitutional, the Court reasoned that sense-enhancing technologies threatened to erode privacy in the home over the long term.[77]

These four models often overlap as judges jump between them while making arguments.[78] In difficult cases, different models will often point judges in different directions.[79] In Kerr's view, a court's challenge is not just to determine whether a model justifies a specific result, but why some models should be used and others discarded in a particular case.

4. Privacy in Location and Movement

Analysis of *Katz* jurisprudence is difficult without reference to certain facts. Therefore, this section considers the application of the *Katz* test to electronic surveillance.

a. Electronic Location Surveillance and the Supreme Court

The first Supreme Court case to address electronic location surveillance was *United States v. Knotts*.[80] In *Knotts*, the police placed a beeper in a five-gallon drum of chloroform.[81] One of the defendants bought the drum, put it in his car, and drove toward a remote cabin.[82] During the drive, the officers maintained visual surveillance until the defendants began evasive maneuvers.[83] The police tracked them to the cabin using the beeper, then

71. *Id.* at 516.
72. *See id.* at 516–17.
73. *Id.* at 517 (citing Florida v. Riley, 488 U.S. 445, 451 (1989)).
74. *See* Kerr, *supra* note 61, at 519.
75. *Id.* ("[T]he policy model presumably plays a guiding hand in many cases even when an opinion itself is framed in terms of the probabilistic model, private facts model, and/or positive law model.").
76. *See id.* at 520.
77. *Id.* (citing Kyllo v. United States, 533 U.S. 27, 40 (2001)).
78. *See* Kerr, *supra* note 61, at 524.
79. *Id.*
80. 460 U.S. 276, 277 (1983).
81. *Id.* at 277 ("A beeper is a radio transmitter . . . which emits periodic signals that can be picked up by a radio receiver.").
82. *Id.*
83. *Id.* at 278.

visually surveilled the property for three days before obtaining a search warrant.[84] The Court ruled that "[a] person travelling in an automobile on public thoroughfares has no reasonable expectation of privacy in his movements from one place to another."[85] Employing a private facts analysis, the Court reasoned that such a person voluntarily conveys the details of his journey to anyone who wants to observe.[86] The beeper was a "scientific enhancement," but it was closely analogous to visual surveillance.[87]

In *United States v. Karo*,[88] agents used the same technique to track a defendant carrying a drum of ether.[89] Unlike *Knotts*, the agents monitored the beeper for days as it was brought inside one defendant's home, then another, and finally to a commercial storage facility.[90] The Court held that entering the home was a search, even though a beeper was less intrusive than physical entry.[91] The beeper revealed a critical fact about the interior that the agents wanted to know and would not have known otherwise[92]: the home contained a drum of ether. The government argued that this requirement would create the need to obtain warrants in all cases, because officers could never predict whether a beeper would enter private premises during tracking.[93] The Court was unsympathetic,[94] but limited it's analysis to when a beeper reveals it is in a *particular* private place.[95] When the police tracked the beeper to the storage facility full of private lockers, they could not identify the particular locker containing the beeper.[96] In that instance, the Court concluded that tracking the beeper was not a search, because the tracking did not intrude on the subject's reasonable expectation of privacy in the locker.[97]

In *Kyllo v. United States*,[98] the Court further reinforced Fourth Amendment protection of the home.[99] Use of extrasensory technology that reveals information about the inside of a house is a search, even if the information is observed from outside its walls;[100] any detail of the home is

84. *Id.* at 278–79.
85. *Id.* at 281.
86. *Id.* at 281–82.
87. *See id.* at 285 ("A police car following [the defendant] at a distance throughout his journey could have observed him leaving the public highway and arriving at the cabin . . . .").
88. 468 U.S. 705 (1984).
89. *See id.* at 708.
90. *Id.*
91. *See id.* at 714–15.
92. *Id.* at 715.
93. *Id.* at 718.
94. *See id.* ("The argument that a warrant requirement would oblige the government to obtain warrants in a large number of cases is hardly a compelling argument against the requirement.").
95. *See id.* at 720.
96. *Id.*
97. *Id.* at 720 n.6.
98. Kyllo v. United States, 533 U.S. 27 (2001).
99. *Id.* at 34.
100. *See id.* at 34–36. In private homes, citizens must retain the same privacy from government that existed when the Fourth Amendment was adopted. *Id.* at 34.

an intimate detail, no matter how seemingly trivial.[101] *Kyllo* further held that courts should take into account future developments when crafting rules to fit new technology.[102]

b. Privacy in Movement over Time: GPS Tracking of Automobiles

The Supreme Court most recently considered the constitutionality of electronic surveillance in *United States v. Jones*.[103] Prior to *Jones*, the federal circuits had split on whether the attachment of a GPS device to a suspect's vehicle and the monitoring of its movement on public streets constituted a search.[104] The Seventh and Ninth Circuits found that GPS tracking was analogous to the beeper tracking in *Knotts*.[105] The D.C. Circuit, however, found that GPS tracking was a search because it grants the government the ability to track the entirety of a person's movements for weeks.[106] While cell phone tracking is factually distinct because phones can enter the home, both issues potentially involve the same question: does the aggregation of information make a police practice more intrusive over time, or should long-term surveillance be treated the same as short-term surveillance?

The Seventh and Ninth Circuits ruled that GPS technology, like the beeper before it, simply makes existing police techniques more efficient.[107] Under *Knotts*, a car's whereabouts on public roads can be tracked because they are willingly exposed to the public.[108] Neither court found that GPS tracking was different enough from the use of a beeper to warrant a departure from *Knotts*.[109] The Eighth Circuit agreed, but limited its holding: a warrant is not required when the police have reasonable suspicion that a particular vehicle is transporting drugs, and the device should only be attached for a reasonable period of time.[110]

In *United States v. Maynard*,[111] the D.C. Circuit departed from this consensus, holding that prolonged, extensive GPS surveillance on public

101. *Id.* at 37.

102. *See id.* at 36.

103. 132 S. Ct. 945 (2012). This section is indebted to Kaitlyn Kerrane's Note on the issue, published in Volume 79 of the *Fordham Law Review*. Kaitlyn A. Kerrane, Note, *Keeping Up with Officer Jones: A Comprehensive Look at the Fourth Amendment and GPS Surveillance*, 79 FORDHAM L. REV. 1695 (2011).

104. Kerrane, *supra* note 103, at 1699.

105. United States v. Pineda-Moreno, 591 F.3d 1212, 1216 (9th Cir. 2010); United States v. Garcia, 474 F.3d 994, 997 (7th Cir. 2007).

106. United States v. Maynard, 615 F.3d 544, 558 (D.C. Cir. 2010), *cert. denied*, 131 S. Ct. 671 (2010), *and aff'd in part sub nom. Jones*, 132 S. Ct. 945.

107. *Pineda-Moreno*, 591 F.3d at 1216; *Garcia*, 474 F.3d at 997.

108. Kerrane, *supra* note 103, at 1723. This public exposure analysis resembles Kerr's "private facts" model of Fourth Amendment privacy. *See supra* notes 68–70 and accompanying text.

109. *Pineda-Moreno*, 591 F.3d at 1216; *Garcia*, 474 F.3d at 997.

110. *See* United States v. Marquez, 605 F.3d 604, 610 (8th Cir. 2010). Both the Seventh and Eighth circuits explained that their holdings would not support a regime of mass surveillance. *Id.*; *Garcia*, 474 F.3d at 998.

111. 615 F.3d 544 (D.C. Cir. 2010), *cert. denied*, 131 S. Ct. 671 (2010), *and aff'd in part sub nom. Jones*, 132 S. Ct. 945.

roads is a search.[112] The court distinguished *Knotts*, writing that month-long GPS tracking exposes the totality of a person's movements in a way that cannot be equated to the visual surveillance of a car during a single trip.[113] While a single trip can be visually surveilled, there is no likelihood that anyone will observe a full month of movements.[114] *Maynard* also considered whether one's movements over the course of a month are "constructively exposed" because each individual movement is in public view.[115] The court held that the whole of a person's movements are not constructively exposed, because the whole of a person's movements reveals more than the sum of its parts.[116] Drawing from other areas of law, the court applied the "mosaic theory" to the Fourth Amendment.[117] Under the mosaic theory, long-term surveillance is a search because it reveals intimate details of a person's life that she reasonably expects no one to observe.[118] The court also distinguished GPS from prolonged visual or photographic surveillance.[119] These traditional methods of surveillance require significant police resources, and this functions as a natural check on government overreach.[120]

The Supreme Court heard *Maynard* on appeal as *Jones*. The Court unanimously held that attaching a GPS device to a suspect's vehicle and monitoring its movement on public streets constituted a search.[121] The majority decided only that a search occurs when the government trespasses on an individual's property for the purpose of gathering information.[122] It left unanswered the question that had split the circuits: whether such tracking would be a search absent a physical trespass. Five justices, however, appeared open to holding that extended tracking is a search even if the government makes no physical contact with an individual's property.[123]

Justice Alito, writing for four concurring justices, criticized the majority for relying on "18th-century tort law."[124] He suggested that reasonable

112. *Id.* at 563.
113. *Id.* at 558.
114. *Id.*
115. *Id.* at 560–62.
116. *Id.* at 562.
117. *Id.* at 562 (citing CIA v. Sims, 471 U.S. 159, 178 (1985)). The mosaic theory is taken from the government's argument in *CIA v. Sims*, 471 U.S. 159 (1985), and other cases involving national security information. The government had argued that it could not reveal seemingly innocuous details because foreign intelligence agencies can assemble useful information from the bits and pieces. *Id.* at 178–79.
118. *Maynard*, 615 F.3d at 563.
119. *Id.* at 565.
120. *Id.* The court likened this distinction to the different approaches the U.S. Supreme Court has taken to warrantless recording of conversations. *Id.* at 566. If the police plant an undercover agent, such recording is permitted. Lopez v. United States, 373 U.S. 427, 429, 440 (1963). The police cannot, however, wiretap a phone without a warrant. *See* Katz v. United States, 389 U.S. 347, 353 (1967).
121. United States v. Jones, 132 S. Ct. 945 (2012).
122. *Id.* at 951 n.5.
123. *See infra* notes 132–36 and accompanying text. The five are Justices Ginsburg, Breyer, Alito, Sotomayor, and Kagan.
124. *Id.* at 957 (Alito, J., concurring).

expectation of privacy should be the sole test used in the case.[125] Applying this standard, he found that the long-term monitoring at issue was a search.[126] He wrote that while short-term monitoring of movements on public streets is acceptable, longer-term monitoring "impinges on expectations of privacy."[127] He emphasized, that in the past, privacy was protected more by technological and practical limitations than by constitutional protection.[128] Society expects that the government will not continually track movements for longs period because it was impossible to do so in the past.[129] In Justice Alito's view, that expectation should be protected against technological advances.[130] The concurrence did not consider at what point monitoring becomes a search, only that four weeks "surely crossed" the line.[131]

Justice Sotomayor joined Justice Scalia's majority opinion applying the trespassory test, but wrote a separate opinion signaling a willingness to apply Justice Alito's analysis in a future case.[132] She characterized the trespassory test as an "irreducible constitutional minimum" and found it sufficient to decide the case.[133] While she rejected Justice Alito's contention that a trespassory analysis should not apply, she agreed that long term monitoring impinges on a reasonable expectation of privacy.[134] She wrote that GPS surveillance allows police to gather a wealth of personal data and to mine it for years.[135] Because tracking is cheap and surreptitious, it is not subject to the ordinary checks on police power: community hostility and a lack of resources.[136]

It now appears that at least five justices stand ready to rule that prolonged tracking is a search.[137] Several commentators have concluded that the Court will endorse some version of the D.C. circuit's mosaic theory.[138] Until then, however, the state of the law remains unclear.[139]

---

125. *Id.* at 958 ("[The trespassory test] strains the language of the Fourth Amendment; it has little if any support in current Fourth Amendment case law; and it is highly artificial. I would analyze the question presented in this case by asking whether respondent's reasonable expectations of privacy were violated by the long-term monitoring of the movements of the vehicle he drove.").

126. *Id.* at 949.

127. *Id.* at 964.

128. *Id.* at 963. ("In the pre-computer age, the greatest protections of privacy were neither constitutional nor statutory, but practical. Traditional surveillance for any extended period of time was difficult and costly and therefore rarely undertaken.").

129. *Id.* at 964. ("For such offenses, society's expectation has been that law enforcement agents and others would not—and indeed, in the main, simply could not—secretly monitor and catalogue every single movement of an individual's car for a very long period.").

130. *See id.*

131. *Id.*

132. *See id.* at 955 (Sotomayor, J., concurring).

133. *Id.*

134. *Id.*

135. *Id.*

136. *Id.*

137. *See supra* notes 132–36 and accompanying text.

138. Orin S. Kerr, *The Mosaic Theory of the Fourth Amendment*, 110 MICH. L. REV. (forthcoming 2012) (manuscript at 2), *available at http://ssrn.com/abstract=2032821* ("The concurring opinions in *Jones* raise the intriguing possibility that a majority of the Supreme

c. Privacy and Cell Phone Tracking

Several courts have considered warrantless cell phone tracking in criminal investigations. Because those cases consider tracking absent any showing of probable cause, they are not directly related to this Note's core issue, but they are useful for understanding how courts view the privacy issues raised by cell phone tracking.

When considering cell phone tracking, many courts have focused on statutory, rather than constitutional, questions. Under federal statute, the government must apply for court orders compelling service providers to disclose customer-tracking data.[140] Some disclosures require probable cause, others a lesser showing; if no federal statute authorized a court order on less than probable cause, a court could reject the government's application on statutory grounds, without need to discuss the Constitution.[141] Under federal law, there are several categories of surveillance.[142] For the least invasive surveillance, like pen registers,[143] the application must only certify that the information likely to be obtained is relevant to an ongoing criminal investigation.[144] Under the Stored Communication Act,[145] access to stored communications, such as subscriber information or account records, requires "specific and articulable facts showing that there are reasonable grounds to believe" that the records sought are "relevant and material."[146] Search warrants, including those for

---

Court is ready to endorse a new mosaic theory of Fourth Amendment protection."); Tom Goldstein, *Why* Jones *Is Still Less of a Pro-privacy Decision Than Most Thought (Conclusion Slightly Revised Jan. 31)*, SCOTUSBLOG (Jan. 30, 2012, 10:53 AM), http://www.scotusblog.com/2012/01/why-jones-is-still-less-of-a-pro-privacy-decision-than-most-thought ("[T]here was seemingly a majority for a more consequential decision holding that long-term monitoring (even by non-physical means) is a search requiring a warrant under the Fourth Amendment.").

139. *See* United States v. Graham, 846 F. Supp. 2d 384, 394 (D. Md. 2012) ("[I]t appears as though a five justice majority is willing to accept the principle that government surveillance over time *can* implicate an individual's reasonable expectation of privacy. However . . . the factual differences between the GPS technology considered in the *Jones* case and the historical cell site location data in the present case lead this Court to proceed with caution in extrapolating too far from the Supreme Court's varied opinions in *Jones*.").

140. *See In re* U.S. for an Order Directing a Provider of Elec. Commc'n Serv. to Disclose Records to Gov't, 620 F.3d 304, 307 (3d Cir. 2010) [hereinafter *Third Circuit CSLI Op.*]

141. *See* Smith Testimony, *supra* note 42, at 82–84 (discussing various magistrate decisions considering the applicable statutes). By contrast, the Constitution itself provides the primary check on actions police can take without a court order. *See, e.g.*, Terry v. Ohio, 392 U.S. 1, 11 (1968). "Triggerfish" can eliminate the need to compel service providers, but they are a recent development. *See supra* notes 37–41 and accompanying text.

142. *See In re* U.S. for and Order: (1) Authorizing Use of a Pen Register & Trap & Trace Device, (2) Authorizing Release of Subscriber & Other Info., (3) Authorizing Disclosure of Location-Based Services, 727 F. Supp. 2d 571, 572 (W.D. Tex. 2010) [hereinafter *2010 W.D. Tex. Op.*].

143. Pen registers are devices installed at a phone company's office that record the numbers dialed from a particular telephone. *See* Smith v. Maryland, 442 U.S. 735, 737 (1979).

144. *2010 W.D. Tex. Op.*, 727 F. Supp. 2d at 572; *see also* 18 U.S.C. § 3122(b)(2) (2006).

145. 18 U.S.C. § 2703(d) (2006).

146. *Id.*

location tracking, require a showing of probable cause.[147] They may only be issued for: (1) evidence of a crime; (2) contraband or fruits of the crime; (3) property designed for use, intended for use, or used in committing a crime; or (4) a person to be arrested or a person who is unlawfully restrained.[148] Even if surveillance falls under a statute requiring less than probable cause, a court can deny an application on constitutional grounds.[149]

Courts have considered three kinds of cell phone tracking: prospective CSLI, historical CSLI, and GPS.[150] The first opinions discussing real-time CSLI began surfacing in 2005.[151] Between 2005 and 2010, the government requested only imprecise, intermittent tracking without showing probable cause.[152] These requests sought information from single cell towers, which could only place users within several hundred feet.[153] The CSLI opinions from this period primarily grappled with statutory questions rather than the Fourth Amendment.[154] Other magistrate opinions, as well as a few district court opinions, surfaced over the next several years.[155] A majority have held that no federal statute authorizes a less-than-probable-cause standard.[156] One judge went further, holding that CSLI violates the Fourth Amendment.[157] A minority of courts held that federal statute allowed a limited form of CSLI: imprecise[158] location tracking, but only when the target made and received calls.[159] The first opinion to adopt this minority view explained that an interaction between three statutes[160] allows ongoing

147. FED. R. CRIM. P. 41(d).

148. *Id.* at R. 41(c). This rule tracks the constitutional analysis of *Warden v. Hayden*, 387 U.S. 294 (1967). *See infra* notes 267–70 and accompanying text.

149. *See Third Circuit CSLI Op.*, 620 F.3d 304, 318–19 (3d Cir. 2010) (holding that, for a magistrate judge to determine whether tracking would reveal information implicating the Fourth Amendment, he or she must be able to determine what information would be disclosed to the government).

150. *See supra* Part I.A.

151. *See, e.g.*, *In re* U.S. for an Order for Disclosure of Telecomm. Records & Authorizing the Use of a Pen Register & Trap & Trace, 405 F. Supp. 2d 435 (S.D.N.Y. 2005) [hereinafter *2005 S.D.N.Y. Opinion*]; *In re* Pen Register & Trap/Trace Device with Cell Site Location Auth., 396 F. Supp. 2d 747 (S.D. Tex. 2005).

152. *See, e.g.*, Brief for United States at 7, *Third Circuit CSLI Op.*, 620 F.3d 304 (No. 08-4227), 2009 WL 3866618 (requesting historical CSLI records).

153. *See, e.g.*, *Third Circuit CSLI Op.*, 620 F.3d at 311; *2010 W.D. Tex. Op.*, 727 F. Supp. 2d 571, 578 (W.D. Tex. 2010).

154. *See* Smith Testimony, *supra* note 42, at 82–83.

155. *See id.*

156. *Id.* at 6; *See, e.g.*, *In re* U.S. for an Order Relating to Target Phone 2, 733 F. Supp. 2d 939, 943 (N.D. Ill. 2009).

157. *See In re* U.S. for an Order Authorizing (1) Installation and Use of a Pen Register & Trap & Trace Device or Process, (2) Access to Customer Records, and (3) Cell Phone Tracking, 441 F. Supp. 2d 816, 837 (S.D. Tex. 2006) ("The constitutional problems created by the [CSLI tracking] are the same, regardless of the breadth of the cell site data sought in a given case.").

158. *See 2005 S.D.N.Y. Opinion*, 405 F. Supp. 2d 435, 438 (S.D.N.Y. 2005) ("[N]o data is provided that could be "triangulated" to permit the precise location of the cell phone user.").

159. *See* Smith Testimony, *supra* note 42, at 84.

160. 18 U.S.C. § 2703 (Supp. V 2011); 18 U.S.C. § 3127(3)–(4) (2006); 47 U.S.C. § 1002 (2006).

CSLI.[161] This approach became known as the "hybrid theory."[162] The hybrid theory opinions that considered the Constitution[163] ruled that the requested CSLI was too imprecise to implicate the Fourth Amendment.[164]

In 2010, the Third Circuit weighed in on historical CSLI.[165] To date, it is the only federal court of appeals to consider the matter. *In re United States for an Order Directing a Provider of Electronic Communication Service to Disclose Records to Government*[166] (*Electronic Communication Service)* held that the Stored Communications Act allows a court to issue an order for CSLI based on a showing of less than probable cause,[167] but that the language of the statute does not prevent a magistrate judge from refusing certain requests on constitutional grounds.[168] It remanded the case, requiring that the magistrate provide a full finding of fact before ruling that a probable cause showing was required.[169]

After the Third Circuit decision, several magistrates held that imprecise, intermittent cell phone tracking is unconstitutional. A district judge in the Southern District of Texas has since affirmed one such opinion, written by Magistrate Judge Stephen Wm. Smith.[170] Judge Smith cited *Maynard* extensively and held that the differences between CSLI and automobile

161. *See 2005 S.D.N.Y. Op.*, 405 F. Supp. 2d at 448.

162. *See, e.g.*, *In re* U.S. for an Order Authorizing the Use of Two Pen Register & Trap & Trace Devices, 632 F. Supp. 2d 202, 205 (E.D.N.Y. 2008).

163. One decision refused to consider the Constitution during the application stage, writing that potential privacy violations from the requested CSLI could be raised in a motion to suppress if the target were indicted. *In re* U.S. for an Order for Prospective Cell Site Location Info. on a Certain Cellular Tel., 460 F. Supp. 2d 448, 462 (S.D.N.Y. 2006).

164. *See, e.g.*, *In re* U.S. for an Order Authorizing the Use of Two Pen Register & Trap & Trace Devices, 632 F. Supp. 2d at 208; *In re* U.S. For an Order: (1) Authorizing the Installation and Use of a Pen Register and Trap and Trace Device; and (2) Authorizing the Release of Subscriber Information and/or Cell Site Info., 411 F. Supp. 2d 678, 682 (W.D. La. 2006).

165. *Third Circuit CSLI Op.*, 620 F.3d 304, 315 (3d Cir. 2010). Some courts have held that requests for historical CSLI should be granted more liberally than real-time CSLI, because historical CSLI is more in line with Congressional intent in passing the Stored Communications Act. *See In re* Pen Register & Trap/Trace Device with Cell Site Location Auth., 396 F. Supp. 2d 747, 760 (S.D. Tex. 2005). Other courts have held that real-time and historical CSLI should be treated identically. *In re* U.S. for an Order for Prospective Cell Site Location Info. on a Certain Cellular Tel., 460 F. Supp. 2d at 459. The Third Circuit seems to suggest its holding applies to both. *Third Circuit CSLI Op.*, 620 F.3d at 315 ("[T]he protections that Congress adopted for CSLI . . . have no apparent relevance to [the Stored Communications Act], and the legislative history does not show that Congress intended to exclude CSLI or other location information from [the Stored Communications Act]."). To the extent the two are factually distinct, real-time CSLI is more relevant to the topic of this Note.

166. 620 F.3d 304 (3d Cir. 2010).

167. *Id.* at 315. The court discussed—but did not adopt—the hybrid theory. *Id.* at 310 n.6.

168. *Id.* at 317. The court also considered the third-party doctrine, discussed *infra* Part I.B.5.

169. *Id.* at 319.

170. *Judge Smith Op.*, 747 F. Supp. 2d 827 (S.D. Tex. 2010). The district court affirmed the magistrate's opinion in one page. *In re* U.S. for Historical Cell Site Data, No. 11-MC-223 (S.D. Tex. Nov. 11, 2011), *available at* http://online.wsj.com/public/resources/documents/hughesorder1116.pdf.

GPS tracking do not merit a different result.[171] He found that CSLI is more invasive than GPS because it is equally accurate and can be monitored indoors where the expectation of privacy is highest.[172] CSLI also reveals more than vehicular GPS because cell phones are on the subject's person.[173]

In at least one case, the government has applied for precise CSLI.[174] The magistrate rejected that application.[175] To date, no published magistrate opinion has approved the use of CSLI that would allow the government to precisely track the movements of a target.[176]

5. Third-Party Doctrine

A person who voluntarily discloses information to a third party loses Fourth Amendment protection of that information. If cell phone location information falls within this "third-party doctrine," government acquisition of that information is not a search. The third-party doctrine applies even if the subject assumed the information would only be used for limited purposes. However, the Supreme Court decisions that established the third-party doctrine are decades old, and it is unclear how the doctrine applies to twenty-first century technology. This section traces the history of the third-party doctrine from its origins to its current application to cell phones.

a. Origins of the Third-Party Doctrine

The Supreme Court held in *United States v. Miller*[177] that individuals have no reasonable expectation of privacy in their bank records.[178] The Court relied on a line of cases challenging the admissibility of statements made to supposed friends and colleagues who later turned out to be government informants.[179] In *Miller*, federal investigators had, without a warrant, subpoenaed the defendant's bank records, which revealed he had written checks to buy equipment used to distill black-market whiskey.[180] The Court observed that the checks were not confidential communications but negotiable instruments containing information voluntarily conveyed to

171. *Judge Smith Op.*, 747 F. Supp. 2d at 838–40. Judge Smith explains two differences: First, automobile GPS is prospective data, and the historical CSLI was recorded. *Id.* at 839. Second, historical CSLI was "neither created nor maintained at the direction of law enforcement," unlike GPS data. *Id.*

172. *Id.* at 840.

173. *Id.*

174. *2010 W.D. Tex. Op.*, 727 F. Supp. 2d 571, 579 (W.D. Tex. 2010).

175. *Id.* at 574–75.

176. Most magistrate judges who have considered this subject have not issued public opinions. *See* Smith Testimony, *supra* note 42, at 84 n.20. It is possible that, despite the absence of authority, some or even most magistrates approve precise CSLI.

177. 425 U.S. 435 (1976).

178. *Id.* at 442.

179. *Id.* at 443. The latest of these was *United States v. White*, 401 U.S. 745 (1971). *White* held that *Katz* did not protect a misplaced belief that the person he confides in will not reveal his wrongdoing. *Id.* at 751–52. For an overview of these "Secret Agent Cases," see Orin S. Kerr, *The Case for the Third-Party Doctrine*, 107 MICH. L. REV. 561, 567–69 (2009).

180. *Miller*, 425 U.S. at 437–38.

banks in the ordinary course of business.[181] *Miller* ruled that by conveying information to another, an individual assumes the risk that the third party will provide that information to the government.[182]

b. Third-Party Doctrine and Electronic Surveillance: Smith v. Maryland

In *Smith v. Maryland*,[183] the Court held that government use of pen registers is constitutional under the third-party doctrine.[184] Officers had used a pen register installed at a phone company's office to record the numbers that the suspect had dialed.[185] The *Smith* Court doubted that people hold a subjective expectation of privacy in their dialed numbers, the first prong of the *Katz* test.[186] The Court wrote that all subscribers realize they must convey numbers to the company to complete a call, and all realize that the company has facilities for making a permanent record of numbers dialed.[187]

The Court acknowledged the limitations of this subjective test, noting that the government could destroy an actual expectation of privacy simply by announcing on national television that it no longer existed.[188] If subjective expectations were made conditional, a normative inquiry would instead be proper.[189] The Court did not actually entertain that argument; it ruled that Smith had no actual expectation of privacy.[190]

Turning to the second prong of the *Katz* test, the Court ruled that any expectation of privacy in numbers dialed would be unreasonable.[191] By exposing numerical information to the telephone company, Smith assumed the risk that the company would turn over that information to the government.[192]

Smith argued that because companies do not make records of local calls for billing, they are not disclosed to the provider.[193] The Court rejected this argument, refusing to "make a crazy quilt of the Fourth Amendment" by basing its holding on the technicalities of a particular phone company's billing practices.[194] The Court observed that the automated switching equipment had taken the place of the human operators responsible for

181. *Id.* at 442.
182. *Id.* at 443.
183. 442 U.S. 735 (1979).
184. *Id.* at 743–44. Neither *Smith* nor *Miller* use the term "third-party doctrine," but scholars have applied the name. *See generally* Stephen E. Henderson, *The Timely Demise of the Fourth Amendment Third Party Doctrine*, 96 IOWA L. REV. BULL. 39 (2011); Kerr, *supra* note 179.
185. *Smith*, 442 U.S. at 737.
186. *Id.* at 742.
187. *Id.*
188. *Id.* at 740 n.5.
189. *Id.*
190. *Id.* at 743.
191. *Id.*
192. *Id.* at 744.
193. *Id.* at 744–45.
194. *Id.* at 745.

routing calls.[195] Smith had conceded that he would have no privacy in numbers conveyed to a human operator, and the Court determined that the company's decision to automate should not create a reasonable expectation of privacy.[196]

c. Third-Party Doctrine in the Twenty-First Century

Smith left open whether the third-party doctrine applies to surveillance technology that is more revealing than pen registers.[197] While its analysis supports a broad application, the *Smith* Court emphasized the limitations of pen register technology and counseled that the specific nature of government activity is important.[198]

Americans disclose much more information to third parties today than in 1979, when *Smith* was decided.[199] Recent cases have considered the privacy of information in email,[200] text messages,[201] Internet Service Provider (ISP) subscriber information,[202] and Twitter accounts.[203] There is little consensus on how to apply *Smith* and *Miller* to recent technological advances. In *City of Ontario v. Quon*,[204] the Supreme Court had a chance to clarify the debate, but it deferred.[205] Rather than decide whether a city employee had a reasonable expectation of privacy in the content of his text messages,[206] the Court assumed *arguendo* that he did and decided the case on other grounds.[207] Justice Kennedy, writing for the majority, cautioned the judiciary not to issue broad opinions about emerging technology before "its role in society has become clear."[208] He added that the ubiquity of cell phones could lead some to consider them necessary instruments for self-identification and self-expression, which would strengthen the case for

195. *Id.* at 744.

196. *Id.* at 744–45.

197. *Id.* at 741–42. The Court noted that the contents of a communication are protected by *Katz*. *Id.* at 741.

198. *Id.* The Court explained that pen registers cannot hear sound, reveal the identities of the callers, or even determine whether the call was completed. *Id.* It is unclear whether these capabilities would have affected the holding, or whether *Smith* or *Katz* applies to information less revealing than the contents of the conversation but more revealing than the numbers dialed.

199. *See* Henderson, *supra* note 184, at 40–44.

200. United States v. Warshak, 631 F.3d 266 (6th Cir. 2010); Rehberg v. Paulk, 611 F.3d 828, 843–46 (11th Cir. 2010), *cert. granted on other grounds*, 131 S. Ct. 1678 (2011); United States v. Forrester, 512 F.3d 500 (9th Cir. 2008).

201. City of Ontario v. Quon, 130 S. Ct. 2619 (2010).

202. United States v. Perrine, 518 F.3d 1196, 1204–05 (10th Cir. 2008); *Forrester*, 512 F.3d at 510.

203. *In re* for an Order Pursuant to 18 U.S.C. § 2703(d), 830 F. Supp. 2d 114 (E.D. Va. 2011).

204. 130 S. Ct. 2619 (2010).

205. *Id.* at 2628–29.

206. The Fourth Amendment applies when the government is acting as an employer. *Id.* at 2627.

207. *Id.* at 2628–29. The reversed Ninth Circuit decision contained an extensive third-party doctrine analysis. Quon v. Arch Wireless Operating Co., 529 F.3d 892, 904–08 (9th Cir. 2008), *rev'd sub nom.* City of Ontario v. Quon, 130 S. Ct. 2619 (2010).

208. *Quon*, 130 S.Ct. at 2629.

protection.[209] But such expectations could be tempered by clearly communicated policies from providers.[210] While the Court evinced no opinion on *Smith*,[211] one commentator heralded *Quon* as signaling the end of the "monolithic" third-party doctrine.[212] This reaction was unsurprising, as opposition to the doctrine among commentators has been nearly unanimous.[213]

In *Jones*, Justice Sotomayor's concurrence criticized the third-party doctrine, calling it "ill suited to the digital age."[214] She expressed doubt that people would accept warrantless government monitoring of their web history just because it was disclosed to a third party for some limited purpose.[215] To protect societal expectations, the Court would need to stop treating secrecy as a prerequisite for privacy.[216] Justice Sotomayor wrote only for herself and explained that deciding the third-party disclosure issue was unnecessary to resolve the case at hand.[217] It remains an open question how the third-party doctrine applies in the digital age.

Two federal circuits have applied the third-party doctrine to email.[218] In *United States v. Forrester*,[219] the Ninth Circuit held that the Fourth Amendment did not protect sender and receiver email addresses.[220] The court found to/from addresses analogous to the numbers dialed in *Smith*: they are used by providers for the specific purpose of routing information, they are voluntarily conveyed, and they do not necessarily reveal anything about the underlying communication.[221] In *United States v. Warshak*,[222] the Sixth Circuit held that the Fourth Amendment protected the contents of email.[223] It emphasized the similarities between emails and letters.

---

209. *Id.* at 2630.

210. *See id.* In *Quon*, the employer provided the phone. *Id.* Justice Kennedy's analysis may not apply if the provider has no employment relationship with the cell phone user.

211. As noted by the Eleventh Circuit, the Supreme Court did not set forth the governing principles necessary to answer the question. Rehberg v. Paulk, 611 F.3d 828, 845 (11th Cir. 2010).

212. *See* Henderson, *supra* note 184, at 41. Justice Scalia, in his concurring opinion, warned as much: "[I]n saying why it is not saying more, the Court says much more than it should." *Quon*, 130 S. Ct. at 2635 (Scalia, J., concurring).

213. *See* Kerr, *supra* note 179, at 564 (citing as examples 1 LAFAVE, *supra* note 59, § 2.7(c), and Daniel J. Solove, *Fourth Amendment Codification and Professor Kerr's Misguided Call for Judicial Deference*, 74 FORDHAM L. REV. 747, 753 (2005)).

214. United States v. Jones, 132 S. Ct. 945, 957 (2012) (Sotomayor, J., concurring).

215. *Id.*

216. *Id.*

217. *Id.*

218. United States v. Warshak, 631 F.3d 266 (6th Cir. 2010); United States v. Forrester, 512 F.3d 500 (9th Cir. 2008).

219. 512 F.3d 500 (9th Cir. 2008).

220. *Id.* at 510. The court also held that the Fourth Amendment does not protect the IP addresses of the sites a user visits or a user's total data usage. *Id.*

221. *Id.* The language excludes information not used to "direct the third party's servers." *See id.* The court explicitly reserved judgment on more intrusive or revealing techniques. *Id.* at 511.

222. 631 F.3d 266 (6th Cir. 2010)

223. *Id.* at 285–86. There were two Sixth Circuit *Warshak* cases, a 2008 civil case and a 2010 criminal case. Casey Perry, Note, *U.S. v. Warshak: Will Fourth Amendment Protection Be Delivered to Your Inbox?*, 12 N.C. J.L. & TECH. 345, 357 n.58 (2011). Each considered

Because the Fourth Amendment protects private communication, *Warshak* held that it must recognize nascent but important media of communication.[224] Neither the ISP's ability, nor its right, to access the email content affected the reasonable expectation of privacy.[225] Anticipating criticism, the *Warshak* court distinguished *Miller*. First, simple business records are different than confidential communications.[226] Second, unlike the bank in *Miller*, the ISP was an intermediary, not the intended recipient of the emails.[227]

From *Quon*, *Forrester*, and *Warshak*, it seems somewhat settled that *Smith* will not apply to the entirety of digital communication. *Smith* remains strong as applied to information analogous to numbers dialed, and *Miller* remains strong as applied to information analogous to bank documents, but neither necessarily controls the wealth of new information disclosed to third parties in the digital age.

d. Third-Party Doctrine and Cell Phone Location

Several cases have considered the third-party doctrine as it relates to cell phones. Whether *Smith* controls cell phone location information depends in part on how police obtained the tracking information.[228] If police cause the phone to emit location information through a GPS ping or other means, *Smith* likely does not apply.[229] *Smith* more plausibly applies when police obtain information that the service provider ordinarily collects when the customer calls or texts. Among circuit courts, only the Third Circuit has considered this issue.[230]

Addressing the issue only briefly, *Electronic Communication Service* held that *Smith* does not apply to historical CSLI.[231] The sharing was not voluntary, because cell phone customers are unlikely to realize that providers collect and store location information.[232] Professor Susan Freiwald predicts that the holding will prove "significant and

---

the application of the third-party doctrine to the contents of email. *See id.* A panel in the civil case ruled that individuals had a privacy interest in their email, but the Sixth Circuit sitting en banc vacated the panel, holding that the issue was unripe for judicial resolution. Warshak v. United States, 532 F.3d 521, 523 (6th Cir. 2008) (en banc). The *Warshak* decision discussed here is the 2010 criminal case.

224. *Warshak*, 631 F.3d at 286.

225. *Id.* at 287. The court observed that in *Katz*, the phone company had the ability to listen in on conversations. *Id.* It also had the legal right to listen to calls to protect itself against the illegal use of its facilities. *Id.* Neither of these considerations gave the government the ability to listen without a warrant in *Katz*. *See id.*

226. *Id.* at 288.

227. *Id.*

228. *See* United States v. Forest, 355 F.3d 942, 951 (6th Cir. 2004), *cert. granted, judgment vacated on other grounds sub nom.* Garner v. United States, 543 U.S. 1050 (2005) (determining that *Smith* does not apply if police dial the subject's cell phone to generate CSLI).

229. *See id.*

230. *Third Circuit CSLI Op.*, 620 F.3d 304 (3d Cir. 2010). This case was discussed *supra* Part I.B.4.c.

231. *Third Circuit CSLI Op.*, 620 F.3d at 317.

232. *Id.*

influential,"[233] but reliance on a lack of customer knowledge has made the precedent vulnerable. For example, a federal judge in Oregon simply concluded that users were aware that companies retained these records.[234] A Louisiana state judge reached the same conclusion after hearing testimony from an AT&T employee that phone bills indicate the tower used to make calls and that the data is used in the ordinary course of business.[235] However, each holding only applied to historical records of imprecise location information.[236] Only one court has fashioned an opinion that could apply to precise, persistent tracking.[237] That court reasoned that pen registers recall mere "notes on a musical scale," while location data is a "grand opera."[238] Professor Freiwald wrote that *Smith* should not apply to all information.[239] Because location tracking exceeds the "limited capabilities" of pen registers, she argued that courts should employ full *Katz* analysis instead of reflexively applying *Smith*.[240] This notion of a middle category between content contained within communications and "limited" information is novel and has not received much consideration by courts or commentators.[241] The application of *Smith* to cell phone tracking remains an open question.

C. Warrants: Requirements, Powers, and Exceptions

The Constitution only prohibits unreasonable searches.[242] Even if precise, persistent tracking constitutes a search within the meaning of the Fourth Amendment, it may nevertheless be constitutional if it is reasonable. Several factors can make a search reasonable, but the primary and preferred method is a warrant supported by probable cause.[243] Armed with an arrest or search warrant, police can reasonably intrude where they otherwise could not. To acquire a warrant, law enforcement officers make a showing of

233. Susan Freiwald, *Cell Phone Location Data and the Fourth Amendment: A Question of Law, Not Fact*, 70 MD. L. REV. 681, 684 (2011).

234. United States v. Davis, Crim. No. 10-339-HA, 2011 WL 2036463, at *3–4 (D. Or. May 24, 2011).

235. State v. Marinello, 49 So. 3d 488, 509–10 (La. Ct. App. 2010).

236. In both, the records disclosed only contained information about a single tower used for each call, preventing triangulation. *Davis*, 2011 WL 2036463, at *4; *Marinello*, 49 So. 3d at 495.

237. *Judge Smith Op.*, 747 F. Supp. 2d 827, 846 (S.D. Tex. 2010), *aff'd In re* U.S. for Historical Cell Site Data, No. 11-MC-223 (S.D. Tex, Nov. 11, 2011), *available at* http://online.wsj.com/public/resources/documents/hughesorder1116.pdf.

238. *Id.* at 846.

239. Freiwald, *supra* note 233, at 741–42.

240. *Id.* at 742.

241. As of the writing of this Note, no court or commentator has considered Professor Freiwald's argument in depth, and the district court affirmed Judge Smith's opinion only within the last year, on November 11, 2011.

242. *See* U.S. CONST. amend. IV.

243. Katz v. United States, 389 U.S. 347, 357 (1967) ("[S]earches conducted outside the judicial process, without prior approval by judge or magistrate, are *per se* unreasonable under the Fourth Amendment—subject only to a few specifically established and well-delineated exceptions.").

probable cause to a magistrate, who authorizes a particular search or seizure.[244]

This section covers several areas of Fourth Amendment warrant law in order to shed light on two issues discussed in Part II. First, what are the requirements for a warrant to search for a person subject to arrest? Second, does *Payton*, which allows police to enter the subject's home without a search warrant to arrest the subject of an arrest warrant, also allow them to track the subject's cell phone?

1. The Probable Cause Requirement

The Fourth Amendment requires that the police have probable cause before executing a search or an arrest.[245] Probable cause is a fluid concept: there are few general principles for determining whether a given set of facts establishes the quantum of evidence necessary to support probable cause.[246] Probable cause exists when the facts would lead a person of reasonable caution to believe that a crime has been, or is being, committed.[247] It requires more than mere suspicion[248] but "significantly lower *quanta* of proof" than necessary to establish guilt.[249] The determination requires an assessment of the totality of the circumstances, operating with probabilities rather than certainties.[250] The facts are viewed from the perspective of a reasonable officer, taking into account training and expertise.[251] Courts determining probable cause require the same quantum of evidence for search and arrest warrants, even though each requires a showing of different facts and circumstances.[252]

2. Search Warrants and Arrest Warrants

To procure an arrest warrant, police must have probable cause to believe that (1) an offense has been committed (2) by the person to be arrested.[253] For a search warrant, police must have probable cause to believe that (1) the items sought are seizable by virtue of their connection with criminal activity, and (2) the items will be found in the place to be searched.[254] There is no requirement that a search warrant name the person whose

244. *Id.*
245. 2 LAFAVE, *supra* note 59, § 3.1(a).
246. *See* Illinois v. Gates, 462 U.S. 213, 232 (1983).
247. Beck v. Ohio, 379 U.S. 89, 96 (1964).
248. Henry v. United States, 361 U.S. 98, 101 (1959).
249. United States v. Davis, 458 F.2d 819, 821 (D.C. Cir. 1972) (citing Draper v. United States, 358 U.S. 307, 311–12 (1959)).
250. *Gates*, 462 U.S. at 230–31 (citing Brinegar v. United States, 338 U.S. 160, 176 (1949)).
251. *See, e.g.*, Klein v. Long, 275 F.3d 544, 550 (6th Cir. 2001); Jackson v. United States, 302 F.2d 194, 196 (D.C. Cir. 1962); United States v. McClard, 333 F. Supp. 158, 164 (E.D. Ark. 1971), *aff'd*, 462 F.2d 488 (8th Cir. 1972).
252. 2 LAFAVE, *supra* note 59, § 3.1(b) (citing Greene v. Reeves, 80 F.3d 1101, 1106 (6th Cir. 1996)).
253. FED. R. CRIM. P. 4(a).
254. *See* 2 LAFAVE, *supra* note 59, § 3.1(b).

property will be searched[255] or persons potentially implicated by the search.[256] Search warrants for tracking devices require a different showing.[257] They must describe the object to be tracked, the circumstances that led agents to want to track the object, and the length of time for which surveillance is requested.[258]

Because the interests protected by the two types of warrants differ, searches involve different procedural protections than arrests.[259] Warrantless arrests are judged by the same probable cause standard as arrest warrants, even if police had time to secure a warrant.[260] By contrast, warrantless searches "are *per se* unreasonable . . . subject to only a few specifically established and well-delineated exceptions."[261] Police inferences must be evaluated by neutral magistrates who, unlike the police, are not engaged in the "often competitive enterprise of ferreting out crime."[262] Officers can delay executing an arrest warrant while they continue to investigate a suspect,[263] but search warrants for tracking devices must specify a reasonable time not exceeding forty-five days in which the device may be used.[264] Officers executing a search warrant can only search for items particularly described in the warrant.[265] They may only search areas that could plausibly contain the items sought.[266]

In *Warden v. Hayden*, the Supreme Court held that officers may search for mere evidence of a crime in addition to instrumentalities, fruits of a crime, or contraband.[267] The Court stated that the Fourth Amendment secures the same level of privacy if a search seeks mere evidence.[268] Only

255. *Id.* (citing United States v. Besase, 521 F.2d 1306, 1308 (6th Cir. 1975)).

256. 2 LAFAVE, *supra* note 59, § 3.1(b) (quoting United States v. McNally, 473 F.2d 934, 941 (3d Cir. 1973)).

257. United States v. Karo, 468 U.S. 705, 718 (1984). Tracking warrants do not seek seizable items and cannot particularly describe a place to be searched. *Id.*

258. *Id.* ("[I]t will still be possible to describe the object into which the beeper is to be placed, the circumstances that led agents to wish to install the beeper, and the length of time for which beeper surveillance is requested. In our view, this information will suffice to permit issuance of a warrant authorizing beeper installation and surveillance.").

259. Steagald v. United States, 451 U.S. 204, 212–13 (1981).

260. *See* Wong Sun v. United States, 371 U.S. 471, 479 (1963).

261. Coolidge v. New Hampshire, 403 U.S. 443, 454–55 (1971).

262. Johnson v. United States, 333 U.S. 10, 14 (1948).

263. *See* United States v. Watson, 423 U.S. 411, 431 (1976) (Powell, J., concurring) ("Good police practice often requires postponing an arrest . . . to place the suspect under surveillance or otherwise develop further evidence necessary to prove guilt to a jury."); *see also, e.g.*, Vafaiyan v. City Of Wichita Falls, Civil No. 7:06-CV-140-O, 2009 WL 3029782, at *1 (N.D. Tex. Sept. 23, 2009) (police delayed executing an arrest warrant and tailed a suspect for three days).

264. FED. R. CRIM. P. 41(e)(2)(C). This is not necessarily a constitutional requirement, however.

265. 2 LAFAVE, *supra* note 58, § 4.6(a) (citing Marron v. United States, 275 U.S. 192, 196 (1927)).

266. *Id.* § 4.10(d) (citing United States v. Chadwell, 427 F. Supp. 692, 696 (D. Del. 1977)).

267. Warden v. Hayden, 387 U.S. 294, 301 (1967). Search and seizure law had been closely tied to property. *Id.* at 303. The government could seize instrumentalities, fruits of crime, or contraband because it had a superior property interest in those items. *Id.* at 303–04.

268. *Id.* at 306–07.

a nexus between the items and criminal activity is required.[269] Put differently, officers must have probable cause to believe that the evidence will aid in apprehension or conviction.[270] Officers can seize any incriminating objects they come across within the proper scope of the search warrant.[271] While search warrants give officers broad power to search private spaces and seize incriminating items, this power is restricted to avoid raising the specter of a general warrant.[272]

3. Probable Cause to Search Arising from Probable Cause to Arrest

Though the quantum of evidence required to secure a search and arrest warrant is the same, probable cause to believe that an individual has committed a crime will not alone support a search warrant.[273] Police can have probable cause to arrest a person without having probable cause to search even the subject's residence.[274] However, if the nature of the crime supports an inference that instrumentalities or other evidence could be found in the subject's residence, then a search warrant for that evidence will issue.[275]

For tracking warrants, it is unclear what, if any, probable cause is required beyond the probable cause to believe that an individual has committed an offense. The Supreme Court has given little guidance on this issue;[276] however, the language of the federal wiretap statute may be instructive.[277] Under the statute, a federal judge may issue a wiretap order if "such interception may provide or has provided evidence of" various crimes.[278] From this language, it appears that tracking warrants, like all warrants, must still seek particular evidence with a nexus to the crime, even though they are not limited to a particular place.

---

269. *Id.* at 307.

270. *Id.*

271. Coolidge v. New Hampshire, 403 U.S. 443, 465 (1971) (describing the "plain view" doctrine); *see also* Horton v. California, 496 U.S. 128, 139 (1990) (noting that officers need not come inadvertently upon incriminating objects not described in the warrant).

272. *Hayden*, 387 U.S. at 301; *see also supra* notes 50–53 and accompanying text (discussing general warrants).

273. 2 LAFAVE, *supra* note 58, § 3.1(b) ("In our opinion an allegation . . . not supported by the facts is insufficient to support [an inference of] criminal activity in a premises, in spite of the fact that there are plenty of allegations alleged to relate to criminal activity of the individual who is alleged to have lived in the premises." (quoting Commonwealth v. Kline, 335 A.2d 361 (Pa. Super. Ct. 1975))).

274. *Id.*

275. *See* United States v. Jones, 994 F.2d 1051, 1056 (3d Cir. 1993) (commenting that stolen cash is the type of loot criminals could hide in their homes); United States v. Lucarz, 430 F.2d 1051, 1055 (9th Cir. 1970) (noting that the suspect had ample time to stash stolen envelopes at home); *see also* United States v. Peacock, 761 F.2d 1313, 1315 (9th Cir. 1985) ("The magistrate need only conclude that it would be reasonable to seek the evidence in the place indicated in the affidavit.").

276. FED. R. CRIM. P. 41(d) advisory committee's note (discussing United States v. Karo, 468 U.S. 705, 718 n.5 (1984)).

277. 18 U.S.C. § 2516 (Supp. V 2011). The standards for wiretapping are quite restrictive. *See id.* This comparison does not imply that tracking is or ought to be subject to the same restriction.

278. *Id.*

4. *Payton v. New York* and the Power of the Arrest Warrant

Police generally need a search warrant to enter a home, but under *Payton*, they can enter for the limited purpose of executing an arrest warrant.[279] *Payton*'s main holding prohibits the police from entering a home to perform a warrantless arrest.[280] The Court also held that an arrest warrant carries the limited authority to enter the suspect's dwelling when there is reason to believe the suspect is within.[281]

Before making a *Payton* arrest, the police can look anywhere in the house where the arrestee might be found.[282] They can also search near the suspect to prevent the concealment or destruction of evidence.[283] Police can conduct a "protective sweep" of the home before or after the arrest.[284] Officers can inspect places from which an attack could be immediately launched, such as adjacent closets.[285] They can search elsewhere if they have a reasonable belief that the area swept harbors an individual posing a danger to the officers or others.[286] The subject of an arrest warrant cannot forestall a protective sweep by stepping outside the home and cooperating, if officers reasonably believe a person within presents a potential threat.[287] The sweep is not a full search, only a "cursory inspection" of certain spaces that ends once the reasonable suspicion has been dispelled.[288] The police must have specific reasons to perform a broad sweep; mere absence of knowledge is insufficient justification.[289] The dominant consideration is the seriousness of the crime being investigated.[290] During a protective sweep, police can seize any evidence in "plain view."[291] Protective sweeps

279. Payton v. New York, 445 U.S. 573, 603 (1980). Police may make an arrest in a public place with or without a warrant. United States v. Watson, 423 U.S. 411, 423 (1976).

280. *Payton*, 445 U.S. at 576.

281. *Id.* at 602–03.

282. Maryland v. Buie, 494 U.S. 325, 330 (1990).

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

284. *Buie*, 494 U.S. at 334.

285. *Id.*

286. *Id.* The federal courts of appeal have split on the showing required under *Payton*'s "reason to believe" requirement. The Ninth Circuit has held that reason to believe requires a showing equivalent to probable cause. United States v. Gorman, 314 F.3d 1105, 1113 (9th Cir. 2002). Every other circuit to consider the issue has held that "reason to believe" requires some lesser showing. Michael A. Rabasca, Note, Payton v. New York*: Is "Reason to Believe" Probable Cause or a Lesser Standard?*, 5 SETON HALL CIRCUIT REV. 437, 445 (2009). Most recently, the Sixth Circuit held that reasonable belief requires "looking at common sense factors and evaluating the totality of the circumstances." United States v. Pruitt, 458 F.3d 477, 482 (6th Cir. 2006).

287. *See* People v. Neutzel, 246 A.D.2d 477, 478 (N.Y. App. Div. 1998).

288. *Buie*, 494 U.S. at 335.

289. *See* United States v. Moran Vargas, 376 F.3d 112, 116 (2d Cir. 2004); United States v. Colbert, 76 F.3d 773, 777–78 (6th Cir. 1996).

290. 3 LAFAVE, *supra* note 58, § 6.4(c) (citing, *e.g.*, United States v. Burrows, 48 F.3d 1011 (7th Cir. 1995)). Some level of individualized suspicion is always required. There is no bright-line rule allowing protective sweeps when arresting violent criminals. *Buie*, 494 U.S. at 334 n.2.

291. Horton v. California, 496 U.S. 128, 135 (1990). "If an article is already in plain view, neither its observation nor its seizure would involve any invasion of privacy." *Id.* at 133.

are common, and the standard for justifying them is often low, but they are not an automatic feature of in-home arrests.[292]

5. Arrests in the Homes of Third Parties: *Steagald v. United States*

Soon after deciding *Payton*, the Court in *Steagald v. United States*[293] considered whether police executing an arrest warrant could enter the homes of third parties to arrest the subject of the warrant.[294] The Court held that an arrest warrant is inadequate to protect the rights of third parties when their homes are searched.[295] The officers' reasonable belief that the suspect was in the third party's home was insufficient to protect the homeowner's procedural rights, because that belief was not subjected to "the detached scrutiny of a judicial officer."[296] A reasonable belief standard would create the potential for abuse for which the post facto remedy of suppression is inadequate.[297] The Court observed that the magistrate requirement furthers the Fourth Amendment's aim: "to prevent, not simply to redress, unlawful police action."[298] With that in mind, *Steagald* required that police obtain a warrant to search the third party's home for the subject of the arrest warrant.[299] Like traditional search warrants, the warrant must particularly describe the place to be searched.[300]

The Court explicitly limited its holding to the rights of third parties, however.[301] The Court did not extend the protection to the subject of the arrest warrant himself, who has no protection.[302] Five circuits have held that *Payton*, not *Steagald*, applies to the subjects of arrest warrants when they are arrested in the homes of third parties.[303]

II. THE CLASH OF PERSPECTIVES OVER THE CONSTITUTIONALITY OF PRECISE, PERSISTENT TRACKING TO FACILITATE ARREST

Part II examines the disagreement over whether police can use cell phone tracking to apprehend the subject of an arrest warrant. Part II.A examines *Specified Wireless Telephone*, a magistrate judge's opinion holding that cell phone tracking violates a reasonable expectation of privacy, that search

292. *See* United States v. Schultz, 818 F. Supp. 1271, 1274 (E.D. Wis. 1993) (holding that protective sweeps cannot be "standard procedure").
293. 451 U.S. 204 (1981).
294. *Id.* at 206.
295. *Id.* at 213.
296. *Id.*
297. *Id.* at 215.
298. *Id.* (quoting Chimel v. California, 395 U.S. 752, 766 n.12 (1969)).
299. *Steagald*, 451 U.S. at 220–21.
300. *See id.* at 214 n.7.
301. *Id.* at 218–19.
302. *Id.*
303. *See* United States v. Jackson, 576 F.3d 465 (7th Cir. 2009); United States v. Agnew, 407 F.3d 193 (3d Cir. 2005); United States v. Kaylor, 877 F.2d 658 (8th Cir. 1989); United States v. Underwood, 717 F.2d 482 (9th Cir. 1983); United States v. Buckner, 717 F.2d 297 (6th Cir. 1983).

warrants for a suspect require probable cause to believe that the suspect is in a particular place, and that *Payton* does not authorize such tracking.

Part II.B considers the opposite perspective. It first analyzes *Bermudez*, in which a district court judge held that *Payton* justifies cell phone tracking if officers have an arrest warrant. Part II.B also includes Professor Orin Kerr's critique of *Specified Wireless Telephone*. Kerr argues that cell phone tracking does not violate the Fourth Amendment, because cell phone location falls under the third-party doctrine and because individuals have no reasonable expectation of privacy in their location or movements. Even if the Fourth Amendment does extend to location information, Kerr maintains that *Payton* and *Steagald* authorize cell phone tracking when police have an arrest warrant.

A. Cell Phone Tracking to Facilitate Arrest Is Held Unconstitutional: Specified Wireless Telephone

On August 3, 2011, Magistrate Judge Gauvey, of the District of Maryland, issued the first and only opinion on the use of precise, persistent cell phone tracking to facilitate arrest: *Specified Wireless Telephone*.[304] While the opinion is not binding precedent, it is notable as the first written consideration of the issue.

1. Procedural History

On June 3, 2010, the United States applied for authorization to ascertain the physical location of the subject's cell phone.[305] The government asked for a GPS ping, along with CSLI for the start and end of any call when precise location was unavailable.[306] At the time of the application, the defendant was unaware of the charges, and the police had not attempted to apprehend him.[307] The government stipulated that the defendant's location was not evidence of a crime, but that the "'requested information [was] necessary to determine the location of [the subject] so that law enforcement officers may execute the arrest warrant [on him].'"[308] The government asked for an order directing the carrier to acquire and disclose location data at specified times or upon the officers' oral request.[309] The requested access would last for thirty days.[310]

The government's request was denied, but the defendant was arrested a few days later.[311] Though the government's request was moot, Judge

304. *Specified Wireless Tel.*, No. 10-2188-SKG, 2011 WL 3423370 (D. Md. Aug. 3, 2011). Because magistrates' rulings need not be written, it is unlikely that Judge Gauvey has been the only magistrate to hear the issue. Nevertheless, hers is the only written opinion.

305. *Id.* at *1.

306. *Id.* For a description of the relevant technologies, see *supra* Part I.A.

307. *Id.* at *2.

308. *Id.* at *1 (quoting the government's application).

309. *Id.*

310. *Id.*

311. *Id.* at *2.

Gauvey noted the issue's importance and invited further argument from the Office of the U.S. Attorney, the U.S. Department of Justice, and the Office of the Federal Public Defender.

2. Privacy in Location and Movement

On August 3, 2011, Judge Gauvey issued an extensive opinion.[312] To determine whether the requested tracking would be a search, the court first laid out the privacy interests at issue.[313] While the government conceded that a subject of an arrest warrant has a reasonable expectation of privacy while in a non-public place, *Specified Wireless Telephone* went further, holding that the subject had a "reasonable expectation of privacy both in his location as revealed by real-time location data and in his movement where his location is subject to continuous tracking over an extended period of time, here thirty days."[314]

The Supreme Court held in *Knotts* that a person has no reasonable expectation of privacy in movements in public areas, regardless of whether surveillance is visual or electronic.[315] Judge Gauvey distinguished cell phone observation from traditional methods because it allows the police "to locate a person entirely divorced from all visual observation."[316] When tracking a phone, officers will not know in advance whether the subject is located in a constitutionally protected place in violation of *Kyllo*,[317] such as a home or even a particular room.[318] Cell phone users keep their cell phones on or close to their person, so placing a cell phone is equivalent to placing its user.[319]

Specified Wireless Telephone also held that the request for "unlimited location data at any time on demand during a thirty-day period" implicated the subject's reasonable expectation of privacy in his movement.[320] The opinion discussed the circuit split over warrantless GPS monitoring of automobiles.[321] While treating *Maynard* with seeming approval, *Specified Wireless Telephone* distinguished cell phone tracking.[322] Unlike

312. *Id.*
313. *Id.* at *8.
314. *Id.* at *9.
315. *Id.* (citing United States v. Knotts, 460 U.S. 276, 281 (1983)).
316. *Id.*
317. *See* Kyllo v. United States, 533 U.S. 27 (2001).
318. *Specified Wireless Tel.*, 2011 WL 3423370, at *9.
319. *Id.* at *10. The opinion cites a Pew study finding that 65 percent of American adults have slept with their cell phone nearby. Amanda Lenhart, *Cell Phones and American Adults*, PEW INTERNET (Sept. 2, 2010), http://www.pewinternet.org/~/media/Files/Reports/2010/PIP_Adults_Cellphones_Report_2010.pdf.
320. *Specified Wireless Tel.*, 2011 WL 3423370, at *11.
321. *Specified Wireless Tel.*, 2011 WL 3423370, at *12. *See supra* Part I.B.4.b.
322. *Specified Wireless Tel.*, 2011 WL 3423370, at *12. While clearly crafting an analysis to survive a reversal of *Maynard*, *Specified Wireless Telephone* does not mention the Supreme Court's grant of certiorari in *United States v. Jones* in its Fourth Amendment analysis. *Jones* is mentioned in the statutory analysis, which this Note does not discuss. *Id.* at *41.

automobiles, she wrote, it is "almost unimaginable" that a cell phone would remain entirely within public spaces.[323]

3. The Reasonability of Precise, Persistent Tracking to Facilitate Arrest

Having decided that cell phone tracking constitutes a search within the meaning of the Fourth Amendment, *Specified Wireless Telephone* next considered whether an arrest warrant makes the search constitutionally reasonable.[324] Relying on *Payton*, the government claimed that where a valid arrest warrant has been issued, it is entitled to "do what it takes to find and arrest the person."[325] Because an arrest warrant authorizes the police to enter a home, it authorizes the lesser infringement of location tracking.[326]

The court rejected this argument, holding that *Payton* requires the government to have a reasonable suspicion that the subject is in a particular place before making an entry.[327] *Specified Wireless Telephone* read *Payton* as a "narrow exception" to the search warrant requirement that only applies if officers can demonstrate a reasonable belief that the suspect "lives at the place to be searched and is present within the place to be searched at the time of arrest."[328] Precise, persistent tracking allows officers to search anywhere for the defendant.[329] The court reasoned that *Steagald*,[330] which declined to extend the *Payton* holding to the homes of third parties, demonstrates that arrest warrants do not give police the ability to enter every dwelling in which they believe the subject is present.[331]

Judge Gauvey observed that the Supreme Court has cited *Payton* seventy-eight times without expanding the holding or applying it to facts similar to those in *Specified Wireless Telephone*.[332] The Court has generally used *Payton* to restrict, not affirm, police conduct.[333] While several circuits have held that the subject of an arrest warrant cannot contest searches in the homes of third parties, such searches still require a reasonable belief that the subject is in a particular place.[334] There is "no doctrinal bridge from the limited authority" to enter a home under *Payton* to the power to obtain "continuous location and movement data" for thirty days.[335] Because tracking provides "different and arguably more" information than a place-based search, Judge Gauvey rejected the

323. *Id.* at *11–12.
324. *See id.* at *14.
325. *Id.* at *13.
326. *Id.*
327. *Id.*
328. *Id.* at *14.
329. *See id.* at *17–18.
330. Steagald v. United States, 451 U.S. 204 (1981).
331. *Specified Wireless Tel.*, 2011 WL 3423370, at *15.
332. *Id.*
333. *Id.* at *16.
334. *Id.* at *16–17 (citing United States v. Jackson, 576 F.3d 465, 468 n.1 (7th Cir. 2009)). Only the owners of the homes can contest such searches. *See supra* notes 301–303.
335. *Specified Wireless Tel.*, 2011 WL 3423370, at *17 (internal quotation marks omitted).

government's claim that cell phone tracking is a "lesser infringement of privacy."[336]

Even if the requested search were limited to "30 days or a reasonable period of time after location of the cell phone and its user to allow a safe arrest, whichever is shorter," cell phone tracking still provides more information than a place-based warrant.[337] The court observed that while entering a person's home need not reveal much information, observing location data over an extended period reveals intimate details of a person's life.[338] Even a search warrant for data at a single moment, which would not implicate privacy of movement, risks invading the privacy of unidentified third parties.[339] This reasoning reflects a particular concern with the investigative potential of cell phone tracking relative to standard *Payton* searches.[340]

4. Authority for a Search Warrant to Aid in Apprehension

Having decided that cell phone tracking is a search and that *Payton* does not allow that search, the *Specified Wireless Telephone* court next considered whether the government had made the required showing of probable cause to obtain a search warrant.[341] The government claimed it could demonstrate that it had probable cause to believe that the "evidence sought will aid in a particular apprehension."[342] The government read *Hayden* to suggest that law enforcement can use a search warrant to aid in the apprehension of a defendant without showing a nexus between criminal behavior and the suspect's movements.[343] The court, agreeing with the public defender, declared the cited language dicta, because the evidence in *Hayden* was used to convict, not apprehend, the defendant.[344] Judge Gauvey highlighted alternate language: "there must be a nexus . . . between the item to be seized and criminal behavior."[345] While *Hayden* allows searches for mere evidence, warrants "must still be specifically tailored to

336. *Id.*
337. *Id.*
338. *Id.* at *18.
339. *Id. Specified Wireless Telephone* considered invading the privacy of third parties with cell phone tracking more severe than a place-based search because the individuals are not as readily identifiable. *Id.*
340. *See id.* at *18–19 ("A *Payton* search informs the government as to whether the subject of the arrest warrant is in his home or in another place that the government had probable cause to believe he is. However, the search anticipated here informs the government on an almost continuous basis where the subject is, at places where the government *lacked* probable cause to believe he was, and with persons about whom the government may have no knowledge.").
341. *Id.* at *24.
342. *Id.* at *26.
343. *Specified Wireless Tel.*, 2011 WL 3423370, at *27. The relevant language in *Hayden*: "Thus in the case of 'mere evidence,' probable cause must be examined in terms of cause to believe that the evidence sought will aid in a particular apprehension or conviction." Warden v. Hayden, 387 U.S. 294, 307 (1967).
344. *Specified Wireless Tel.*, 2011 WL 3423370, at *27.
345. *Id.*

permit search or seizure only of things and places that have a connection to the alleged criminal activity."[346]

The government can acquire a search warrant to apprehend a criminal defendant, but it must demonstrate probable cause that the defendant was in a *particular place*.[347] The government could not request "broad information" about the defendant's movements without proving a nexus between those movements and the crime itself.[348] Such authority would be "akin to general investigatory activity, for which search warrants are not issued."[349]

In short, *Specified Wireless Telephone* denied the government's application because precise persistent tracking violated the subject's reasonable expectation of privacy. Judge Gauvey rejected the government's two arguments: that *Payton* justified tracking to facilitate arrest, or in the alternative, that a search warrant could issue where there was probable cause to believe that location information would aid in the apprehension of the subject.

B. Cell Phone Tracking to Facilitate Arrest Is Constitutional

This section examines the opposition to *Specified Wireless Telephone*. It analyzes *Bermudez*, which held that imprecise tracking is allowed under *Payton*, and explains Orin Kerr's criticism of *Specified Wireless Telephone*.

1. Applying Payton to CSLI: *United States v. Bermudez*

In 2006, five years before Judge Gauvey's decision rejecting precise persistent tracking to facilitate arrest, *Bermudez* held that law enforcement could use CSLI to help apprehend the subject of an arrest warrant.[350] In *Bermudez*, the police tracked a phone for less than one day using imprecise, intermittent tracking.[351] The court held that *Payton* allowed cell phone tracking because it was a lesser intrusion into the home than physical entry.[352] The court also held that tracking a cell phone to an area containing a home is constitutional so long as it does not reveal the particular home in which the phone is located.[353] Lastly, the court held that the third-party doctrine allows police to call a phone and use its ring to locate it.[354]

346. *Id.* at *28.
347. *Id.* at *29–30.
348. *Id.* at *30.
349. *Id.*
350. United States v. Bermudez, No. IP 05-43-CR-B/F, 2006 WL 3197181, at *11 (S.D. Ind. June 30, 2006).
351. *Id.* at *1.
352. *Id.* at *10.
353. *Id.* at *12–13.
354. *Id.* at *13.

a. Procedural History

On May 9, 2005, police used real-time CSLI of a phone "believed to be used by or otherwise connected" to a fugitive and tracked the phone to an apartment he had rented.[355] Later that day, officers surveilling the apartment noticed a car driven by two men, one of whom the officers believed to be the fugitive. After observing suspicious behavior, the police stopped the men and arrested one of them, Amaral-Estrada, whom the police believed to be the fugitive.[356]

The police then attempted a consent search of the fugitive's apartment, which the fugitive's mother and her husband, defendant Lira-Esquivel occupied.[357] They called the phone they had been tracking, which was on a table in the apartment.[358] Eventually, the police arrested both Lira-Esquivel and the fugitive's mother. The police did not charge the fugitive's mother, but did charge Amaral-Estrada and Lira-Esquivel with conspiracy to possess with intent to distribute narcotics.[359]

Defendant Lira-Esquivel moved to suppress evidence obtained from the apartment, alleging that the offers exceeded their authority under statute and the Constitution by tracking the cell phone located in his apartment.[360]

b. Application of Payton *to Cell Phone Tracking*

Bermudez first considered whether *Payton* allowed cell phone tracking within a home.[361] The court reasoned that because *Payton* gives police the authority to physically enter the home of the target, it also provides the authority to use less intrusive means to search for the person sought.[362] Therefore, the court determined that tracking a cell phone into a private space is less intrusive than a *Payton* search because it does not involve physical entry.[363] The court did not consider whether the suspect could have a reasonable expectation of privacy in his movements.[364]

---

355. *Id.* at *1. The fugitive, Sosa-Verdeja, was not among those investigated or charged. The tracking was authorized by a court order issued May 3, 2005. *Id.* A fugitive is one who could be or is charged with flight to evade prosecution or testimony under 18 U.S.C. § 1073 (Supp. V 2011). *Specified Wireless Tel.*, 10-2188-SKG, 2011 WL 3423370, at *7 (D. Md. Aug. 3, 2011).

356. *Bermudez*, 2006 WL 3197181, at *2–3.

357. *Id.* at *4.

358. *Id.*

359. *Id.* at *5.

360. *Id.* at *6. Lira-Esquivel also moved to suppress on statutory grounds. The court held that the police had violated the Stored Communications Act and the Pen/Trap Act but that suppression was not an available remedy for violation of those statutes. *Id.* at *7–9.

361. *Id.* at *10–11.

362. *Id.* at *10.

363. *See id.* at *11.

364. *Bermudez* predated the circuit split over GPS tracking of automobiles. The Seventh Circuit subsequently ruled that tracking of automobile movements is not a search. United States v. Garcia, 474 F.3d 994, 997 (7th Cir. 2007). The single day of imprecise, intermittent tracking at issue in *Bermudez* would probably not have been a search under *Maynard*. *See* United States v. Maynard, 615 F.3d 544, 560–63. (D.C. Cir. 2010) (explaining

c. Constitutionality of Tracking a Cell Phone to a Home

In the alternative, Lira-Esquivel argued that the fugitive's cell phone had provided information about his dwelling that the police could not otherwise have obtained, in violation of *Kyllo*.[365] The court disagreed.[366] In *Kyllo*, officers targeted the home to gain information about the activities inside.[367] But in *Bermudez*, police targeted the phone only as to its location and learned only that the phone was in one of three apartment units in a building.[368] And though the signal originated from the home, it could be monitored from outside without revealing information about the home itself.[369]

In a footnote, *Bermudez* cites *Karo* for support.[370] Because the building contained three apartments, it resembled *Karo*'s group of lockers.[371] Police did not intrude on a reasonable expectation of privacy if they could not place the phone within a particular apartment.[372] *Bermudez* also notes that *Karo* explicitly left open whether probable cause is required before monitoring a beeper in a private residence.[373]

d. Third-Party Doctrine

Bermudez further concluded that at least some cell phone signals fell under the third-party doctrine.[374] The court held that officers can call a phone and use its ring to determine its location, even within a home.[375] Because the phone's signals were "knowingly exposed" to the cell phone company, a police officer could call it. If one intends to keep a cell phone's location private, he can just turn it off.[376]

Bermudez only considered imprecise tracking for a short period, but its application of *Payton* contradicts *Specified Wireless Telephone*. While *Bermudez* considered tracking less intrusive than a physical entry,[377] unlike

---

the difference between a whole month of tracking and the tracking of individual movements).

365. *Bermudez*, 2006 WL 3197181, at *12. The Court also held that Lira-Esquivel did not have standing to challenge the tracking of another person's cell phone into his apartment. *Id.* at *11–12 (citing Elk Grove Unified Sch. Dist. v. Newdow, 542 U.S. 1, 15 (2004)).

366. *Bermudez*, 2006 WL 3197181, at *13.

367. *Id.*

368. *Id.*

369. *Id.*

370. *Id.* at *13 n.27.

371. *See id.*

372. *See id.* at *13.

373. *Id.* at *13 n.27.

374. *Id.* at *12–13.

375. *Id.* There is some ambiguity as to whether the court is discussing the dialing or the tracking that preceded it. Because only the ring actually placed the phone *within* the apartment, the court was likely considering the dialing. *Id.* The judge also notes that the Sixth Circuit ruled that CSLI is not voluntarily conveyed in *United States v. Forest*, 355 F.3d 942, 951–52 (6th Cir. 2004), and does not appear to contradict that holding. *Bermudez*, 2006 WL 3197181, at *12–13.

376. *Id.* at *13.

377. *See supra* notes 361–64 and accompanying text.

Specified Wireless Telephone, it did not consider the information-gathering potential of cell phone tracking.

2. Orin Kerr's Objections to *Specified Wireless Telephone*

Soon after *Specified Wireless Telephone* was published, Orin Kerr posted a summary and critique of the opinion on the Volokh Conspiracy.[378] Calling the opinion "pretty clearly wrong," he presented three arguments against it.[379] Kerr argued that the third-party doctrine applies to cell phone location information, that there is no right to privacy in location or movement, and that *Payton* allows police to find a suspect's phone.[380]

a. Third-Party Doctrine Applies to Cell Phone Location Information

Kerr wrote that *Smith v. Maryland* applies to cell phone location information.[381] CSLI is "closely analogous to the numbers dialed in *Smith*"[382] because it is necessary for placing a call and is necessarily transmitted to the service provider.[383] He argues that courts should presume that users know how their cell phones work, much as *Smith* presumed that users knew how landline telephones worked.[384] In his view, it is basic knowledge that cell phones communicate with nearby cell towers to make calls, and failure to have this basic understanding of technology should not provide Fourth Amendment protection.[385] He also observed that the percentage of users with this basic understanding constantly increases.[386] In an earlier post, Kerr had noted that the Sixth Circuit's decision in *Warshak*[387] did not grant protection to CSLI.[388] The panel opinion applied to the contents of an email, but Kerr categorized CSLI as a noncontent record.[389] Because Kerr determined that *Smith* applies, he

378. Orin Kerr, *Court Rules That Police Cannot Use Warrants to Obtain Cell Phone Location of Person Who is Subject of Arrest Warrant*, VOLOKH CONSPIRACY (Aug. 8, 2011, 8:36 PM), http://volokh.com/2011/08/08/court-rules-that-police-cannot-use-warrants-to-obtain-cell-phone-location-of-person-who-is-subject-of-arrest-warrant/. Kerr's post provides links to some of his past arguments about cell phone tracking.

379. *Id.*

380. *Id.*

381. *Id.*

382. Orin Kerr, *Legal Protection for Historical Cell-Site Records*, VOLOKH CONSPIRACY (Feb. 3, 2010, 1:22 AM), http://volokh.com/2010/02/03/legal-protection-for-historical-cell-site-records/ (citing Smith v. Maryland, 442 U.S. 735 (1979)).

383. *Id.*

384. *Id.* (citing *Smith*, 442 U.S. at 742).

385. *Id.*

386. *Id.*

387. *See supra* notes 223–26 and accompanying text.

388. Orin Kerr, *Fourth Amendment Stunner: Judge Rules That Cell-Site Data Protected by Fourth Amendment Warrant Requirement*, VOLOKH CONSPIRACY (Aug. 31, 2010, 2:46 AM), http://www.volokh.com/2010/08/31/fourth-amendment-stunner-judge-rules-that-cell-site-data-protected-by-fourth-amendment-warrant-requirement/.

389. *Id.* Kerr also observed that the 2008 *Warshak* decision had been vacated. He wrote before the 2010 *Warshak* decision, which also held that the contents of emails were protected. *See supra* note 223.

concluded that CSLI is not protected by the Fourth Amendment.[390] Kerr's analysis in this earlier post applied to the historical CSLI considered by the Third Circuit in *Electronic Communication Service*.[391] By linking this analysis to his objection to *Specified Wireless Telephone*, Kerr implied that the same analysis applies to GPS pings and CSLI collected without the placement of a call.

b. The Fourth Amendment Does Not Protect Privacy in Location and Movement

Kerr argued that courts should not deal in abstractions like privacy in location and movement.[392] Instead, courts should ask "whether the particular data stored in a particular place on a particular server is protected."[393] He criticized Judge Gauvey for her overreliance on *Maynard*'s mosaic theory.[394] In other posts, Kerr had argued that *Maynard* introduces a novel, unpersuasive theory of the Fourth Amendment.[395] First, he argued that *Knotts* directly applies to GPS.[396] In *Maynard*, the D.C. Circuit applied the probabilistic model,[397] arguing that it is unlikely that a stranger would monitor the entirety of a suspect's movements.[398] *Knotts* applies the private facts model[399] to electronic surveillance, which Kerr argued is more workable for evaluating technological surveillance.[400] In the private facts model, the nature of the information is relevant, regardless of the technology used to acquire it.[401]

Second, *Maynard* changed the Fourth Amendment inquiry from whether a particular act is a search to whether an entire course of conduct is a search, without any supporting precedent.[402] This approach creates a line-drawing problem: neither police nor the lower courts will know when a set of non-searches becomes a search.[403] In Kerr's view, *Maynard* was wrongly decided, so Judge Gauvey's reliance on it is problematic.[404]

---

390. Kerr, *supra* note 388.
391. Kerr, *supra* note 382.
392. *Id.*
393. Kerr, *supra* note 378.
394. *Id.*
395. Orin Kerr, *D.C. Circuit Introduces "Mosaic Theory" of Fourth Amendment, Holds GPS Monitoring a Fourth Amendment Search*, VOLOKH CONSPIRACY (Aug. 6, 2010, 2:46 PM), http://volokh.com/2010/08/06/d-c-circuit-introduces-mosaic-theory-of-fourth-amendment-holds-gps-monitoring-a-fourth-amendment-search/ (citing United States v. Maynard, 615 F.3d 544 (D.C. Cir. 2010)).
396. Orin Kerr, *Does the Fourth Amendment Prohibit Warrantless GPS Surveillance?*, VOLOKH CONSPIRACY (Dec. 13, 2009, 9:46 PM), http://volokh.com/2009/12/13/does-the-fourth-amendment-prohibit-warrantless-gps-surveillance/ (citing United States v. Knotts, 460 U.S. 276 (1983)).
397. *See supra* notes 65–67 and accompanying text.
398. *See supra* notes 113–20 and accompanying text.
399. *See supra* notes 68–70 and accompanying text.
400. Kerr, *supra* note 396.
401. *Id.*
402. Kerr, *supra* note 395.
403. *Id.*
404. *See* Kerr, *supra* note 378.

c. Payton *and* Steagald *Allow a Search Warrant to Apprehend the Subject of an Arrest Warrant*

Kerr is less convinced about the application of *Payton* and *Steagald* to tracking, calling the question "interesting" and "difficult."[405] He considers it strange that an arrest warrant could allow police to break into a suspect's home but not allow them to locate the suspect's phone.[406] He objects to Judge Gauvey's observation that location tracking would be a novel extension of *Payton*.[407] The application of *Payton* is only novel, Kerr argues, because Fourth Amendment protection of a location is a novel theory.[408]

Kerr suggests that *Steagald* may be read to allow a warrant for tracking.[409] *Steagald* requires that police obtain a search warrant to search the homes of third parties for the subject of an arrest warrant.[410] In Kerr's view, *Steagald*'s search warrant requirement is focused on the government's need to justify the intrusion.[411] The warrant requirement protects the Fourth Amendment rights of the third parties.[412] The same logic supports a search of a phone company's computer to determine the suspect's whereabouts.[413] If the government can justify this imposition to a magistrate, the rights of third parties are protected.[414]

In short, Professor Kerr disagrees with *Specified Wireless Telephone* on both relevant questions. Kerr argues that precise, persistent cell phone tracking is not a search, but that it would be reasonable if it were.[415] Because he rejects *Maynard*'s mosaic theory, he argues that cell phone tracking is not a search.[416] He also argues that cell phone location is unprotected under *Smith* because it is voluntarily disclosed noncontent information.[417] Even if precise, persistent tracking were a search, Kerr believes it would be reasonable under *Payton* if police used it to apprehend the subject of an arrest warrant.[418] He agrees with *Bermudez* that tracking is a lesser intrusion than physical entry into the home and argues that *Steagald* provides police with the ability to acquire a search warrant to aid in locating and arresting the subject of an arrest warrant.[419]

---

405. *See id.*
406. *Id.* (citing Payton v. New York, 445 U.S. 573 (1980)).
407. *Id.*
408. *Id.*
409. *Id.* (citing Steagald v. United States, 451 U.S. 204 (1981)).
410. *Id.*
411. *Id.*
412. *Id.*
413. *Id.*
414. *See id.*
415. *See supra* notes 380–414 and accompanying text.
416. *See supra* notes 392–404 and accompanying text.
417. *See supra* notes 381–91 and accompanying text.
418. *See supra* notes 405–14 and accompanying text.
419. *See supra* notes 405–14 and accompanying text.

III. COURTS SHOULD AUTHORIZE PRECISE, PERSISTENT TRACKING FOR THE LIMITED PURPOSE OF APPREHENDING THE SUBJECT OF AN ARREST WARRANT

Cell phone tracking is a search that should be permitted solely to facilitate the arrest. Courts should allow tracking for the short time necessary to effect arrest, preventing the use of such tracking for investigative purposes.

A. Persistent Precision Tracking Is a Search

This section argues that precise, persistent tracking is a search. It first argues that cell phone tracking violates a reasonable expectation of privacy by revealing intimate details of the subject's movement in both private and public spaces. It further argues that the third-party doctrine should not apply to cell phone location information.

1. Cell Phone Tracking Potentially Violates Privacy in Movement and Location

Precise, persistent tracking can result in two distinct types of searches. First, tracking over extended periods can reveal intimate details about the subject's life.[420] Because rules must account for foreseeable technological advances,[421] courts should treat tracking as if it provides the subject's exact location, even inside private spaces.[422] As Judge Gauvey observed, cell phone tracking implicates privacy concerns similar to the automobile tracking in *Maynard*, the D.C. Circuit ruling that preceded and survived *Jones*.[423] Both Judge Gauvey and the *Maynard* court wrote that the aggregation of location information over time could reveal intimate details of the subject's life,[424] but because precisely tracking a cell phone also penetrates private spaces, the issue is distinct.[425] The GPS tracking in *Jones* aggregated only movements on public roads.[426] Precise, persistent tracking of a cell phone reveals movement in both public and private spaces, including a subject's own home.[427]

Kerr's criticism that Judge Gauvey overrelies on the *Maynard* holding is misplaced.[428] *Maynard* held that otherwise-legal police activity could become a search over time.[429] Precise, persistent cell phone tracking is a collection of searches and nonsearches that become more intrusive over time. Judge Gauvey could have employed the "mosaic" logic of *Maynard*

420. *See supra* notes 116–18 and accompanying text.
421. Kyllo v. United States, 533 U.S. 27, 36 (2001).
422. Cell phone tracking is, or will soon be, virtually exact. *See supra* note 23 and accompanying text.
423. *See supra* notes 321–24 and accompanying text.
424. *See supra* notes 112–18 and accompanying text.
425. *See supra* notes 322–24 and accompanying text.
426. *See supra* notes 112–15 and accompanying text.
427. *See supra* notes 317–24 and accompanying text.
428. *See supra* note 394 and accompanying text.
429. *See supra* notes 112–16 and accompanying text.

without relying on the holding. And unlike the tracking in *Jones*, cell phone tracking is not analogous to any acceptable police activity. GPS tracking resembles tailing vehicles and mass videotaping, but no preexisting police practice enables surveillance of all movements, public and private.[430] The *Jones* decision strengthened Judge Gauvey's position, as it appears that the mosaic theory has traction with at least five justices.[431]

More importantly, precise persistent cell phone tracking reveals private facts.[432] The Court often uses the "private facts" model to evaluate new forms of electronic surveillance.[433] *Knotts* turned primarily on this consideration. Individuals should, however, have a reasonable expectation of privacy in their location and movements within private spaces. This principle underlies *Katz*: entering a private space creates the expectation that others will not intrude.[434] It is no less applicable to tracking movement than it is to video or audio surveillance. Combining these private facts with public surveillance reveals more intimate details than the surveillance in *Jones*. Precise, persistent cell phone tracking also provides considerably more information: it reveals a person's location at all times, not just when he or she is driving.

Maynard and Justice Alito's *Jones* concurrence do not suggest that all GPS surveillance of automobiles is a search.[435] Rather, GPS surveillance for a sustained period *can become* a search if done long enough to create a "mosaic," revealing intimate details of the subject's life.[436] While precise, persistent tracking of a cell phone will likely construct a mosaic much faster than would GPS tracking of an automobile,[437] it does not reveal intimate details instantaneously. This distinction is particularly relevant when considering cell phone tracking to facilitate an arrest. In many cases, the arrest will happen quickly enough that no intimate details are revealed.[438] In *Bermudez*, police made the arrest the same day they began tracking the subject.[439] In cases like *Bermudez*, precise, persistent tracking is not a search under a mosaic analysis.

Tracking need not construct a mosaic to be a search, however. Tracking a cell phone within a home is always a search, regardless of what that

430. *See supra* note 120 and accompanying text.
431. *See supra* note 138 and accompanying text.
432. *See supra* notes 68–70 and accompanying text.
433. *See supra* note 70 and accompanying text.
434. Katz v. United States, 389 U.S. 347, 352 (1967) ("But what he sought to exclude when he entered the booth was not the intruding eye—it was the uninvited ear.").
435. *See supra* notes 112–16, 124–31 and accompanying text.
436. *See supra* notes 112–18 and accompanying text.
437. Cell phone tracking can reveal twenty-four hours of activity in both public and private places. GPS tracking can only reveal the places an individual travels on public roads. It follows that cell phone tracking could reveal an intimate picture of one's life in fewer days of tracking.
438. United States v. Bermudez, No. IP 05-43-CR-B/F, 2006 WL 3197181, at *1 (S.D. Ind. June 30, 2006).
439. *See id.*

tracking reveals.[440] The home is sacrosanct in Fourth Amendment law: all details of the home are intimate details.[441] Judge Gauvey's analysis is correct; precise, persistent tracking is analogous to the searches in *Kyllo* and *Karo*. The *Bermudez* court examined 2006 location technology, which placed the phone within a building but not a particular residence.[442] The tracking in *Bermudez* resembled the group of lockers in *Karo*, but *Karo* explicitly declared that precision tracking within the home is a search.[443] Precise cell phone tracking, like a beeper, reveals critical facts about the home's interior.[444]

The *Bermudez* dicta observing that *Karo* left open whether probable cause should be required is somewhat misleading. *Karo* held that beeper tracking is a search[445] and refused to depart from the warrant requirement.[446] In a footnote at the very end of the analysis, the Court explained that the issue of whether *reasonable suspicion* could justify the search was not before the Court and could be resolved in another case.[447]

Under *Kyllo* and *Karo*, precise, persistent tracking within a home is a search because it reveals details of a home.[448] Such searches require probable cause unless they fall under an existing exception to that requirement.[449] Precise, persistent cell phone tracking thus involves two types of potential searches: "mosaic" searches and *Karo* searches.

2. The Third-Party Doctrine Should Not Apply to Cell Phone Location

Under *Smith* and *Miller*, there is no reasonable expectation of privacy in information voluntarily transmitted to third parties.[450] If *Smith* and *Miller* apply to precise, persistent tracking, it is not a search. In her order, Judge Gauvey did not address the third-party doctrine.[451] She may have considered the issue settled by the Third Circuit in *Electronic Communication Service*.[452] *Bermudez*, decided before the Third Circuit ruled, held that *Smith* could apply to cell phones, because the signal is "knowingly exposed" to third parties.[453] However, *Bermudez* considered the constitutionality of an officer calling a phone to hear it ring, not the constitutionality of tracking.[454] This action falls within Kerr's "positive

440. *See Specified Wireless Tel.*, No. 10-2188-SKG, 2011 WL 3423370, at *9 (D. Md. Aug. 3, 2011).
441. Kyllo v. United States, 533 U.S. 27, 38 (2001).
442. *See supra* notes 368–72 and accompanying text.
443. *See supra* notes 90–95 and accompanying text.
444. *See supra* note 92 and accompanying text.
445. United States v. Karo, 468 U.S. 705, 717 (1984).
446. *Id.* at 717–18.
447. *Id.* at 718 n.5.
448. *See supra* notes 90–102 and accompanying text.
449. *Karo*, 468 U.S. at 717–18.
450. *See supra* notes 178–90 and accompanying text.
451. *See supra* Part II.A.
452. *See supra* notes 231–32 and accompanying text.
453. *See supra* note 376 and accompanying text.
454. United States v. Bermudez, No. IP 05-43-CR-B/F, 2006 WL 3197181, at *13 (S.D. Ind. June 30, 2006).

law" model.[455] By calling the phone, an officer does not exceed the abilities of a private citizen. In turning on their phones, individuals allow any third party to call them. By contrast, location tracking exceeds the ability of the ordinary citizen.

No court has suggested that precise, persistent tracking should fall under *Smith*, but in his critique of Judge Gauvey's opinion, Professor Kerr argues that cell phone location is unprotected.[456] To track a phone in small intervals, police do not rely on the voluntary action of the users. While Professor Kerr's critique asserts that *Smith* applies to all location information, his substantive argument only addresses CSLI generated when the user makes a call.[457] It would stretch *Smith* past plausibility to argue that users voluntarily disclose their location to third parties merely by carrying a cell phone that can be tracked with GPS.

Kerr's actual claim seems to be that police should have access to location information recorded in the ordinary course of business.[458] Like the information in *Smith* and *Miller*, he argues, CSLI is voluntarily revealed by the user and is an essential part of placing a cell phone call.[459] The Third Circuit, the only court of appeals to consider the issue, has ruled that *Smith* does not apply, because cell phone users do not know that their location is disclosed to the service provider.[460]

But by relying on consumers' continued ignorance, the Third Circuit has set a weak precedent.[461] Some courts have already contradicted its holding.[462] As Kerr observes, more users understand the rudiments of the technology with every passing day.[463] And Congress or the Federal Communications Commission could easily circumvent the Third Circuit by mandating some form of disclosure on phone packaging or materials.

The country would benefit from a strong Supreme Court opinion on the third-party doctrine. To have such ambiguity and inconsistency in a major area of privacy law is a problem. Ambiguity is particularly unfortunate in a doctrine declaring that individuals assume the risk that the government will access information they disclose to third parties.[464] If the Court determines that technology users assume the risk of disclosure, then the Court ought to inform them what risks they are assuming.

Smith and *Miller* should not apply to *all* information disclosed to third parties. Each was limited to a specific kind of information. Bank records, while detailed and potentially revelatory, are business documents.[465] The

455. See *supra* notes 71–73 and accompanying text for a description of the positive law model.
456. *See supra* Part II.B.2.
457. *See supra* Part II.B.2.a.
458. *See supra* Part II.B.2.a.
459. *See supra* notes 382–84 and accompanying text.
460. *See supra* notes 231–32 and accompanying text.
461. *See supra* notes 233–36 and accompanying text.
462. *See supra* notes 233–36 and accompanying text.
463. *See supra* note 386 and accompanying text.
464. Smith v. Maryland, 442 U.S. 735, 744 (1979).
465. United States v. Miller, 425 U.S. 435, 442 (1976).

Fourth Amendment, which protects people in their homes and effects, offers greater protection to personal information than it does to business information.[466] Location information, particularly within private spaces, is personal information that should be afforded more protection than business records.

Smith applies to personal information, but the opinion emphasizes the limited capability of the pen register technology at issue.[467] While a pen register cannot even tell if a call is completed, CSLI reveals the number dialed, the length of the call, and the user's location. Numbers dialed are revelatory, but not nearly as revelatory as CSLI. *Warshak* supports the proposition that individuals have a reasonable expectation of privacy in the contents of communications disclosed to intermediaries.[468] Courts should go further. Individuals should have a reasonable expectation of privacy in all but the sort of limited information considered in *Smith*: phone numbers, email to/from addresses, and their direct factual analogues.

In the past, the distinction between content and noncontent was helpful, because no court had considered a form of information that fell between the categories of content and limited information.[469] *Smith* explicitly limited its holding to pen registers, but its argument contains expansive language that courts have applied to a variety of information.[470]

As Justice Sotomayor argued in *Jones*, that approach is "ill suited to the digital age."[471] *Smith* was essentially a backward-looking decision.[472] It gave great weight to the replacement of human operators by automatic switching boards.[473] It certainly did not contemplate the wide swaths of American life that would take place in the digital sphere. As Judge Kennedy wrote in *Quon*, much of the technology that requires third party disclosure could become essential self-expression and self-identity.[474] Cell phones are the paradigmatic example. *Smith* contemplated a world in which a human operator facilitated telephone calls and could memorize the numbers dialed for use in subsequent questioning.[475] Cell phone users disclose much more detailed information.[476] While a list of all numbers dialed is revealing, even intermittent CSLI provides a comprehensive picture of a user's life.

Judge Smith and Professor Freiwald, who write that CSLI falls outside of the third-party doctrine, provide the correct approach.[477] *Smith* did not

466. *See id.* at 440.
467. *See supra* note 198 and accompanying text.
468. United States v. Warshak, 631 F.3d 266, 288 (6th Cir. 2010).
469. *See supra* Part I.B.5.
470. *See supra* Part I.B.5.
471. United States v. Jones, 132 S. Ct. 945, 957 (2012).
472. *See supra* Part I.B.5.b.
473. *See supra* notes 195–96 and accompanying text.
474. *See supra* notes 208–09 and accompanying text.
475. *See supra* notes 195–96 and accompanying text.
476. *See supra* note 238 and accompanying text.
477. *See supra* notes 237–40 and accompanying text.

establish an absolute binary between content and noncontent.[478] It only acknowledges that there is some information that is unprotected if disclosed to a third party, and some information that remains protected.[479] There is no reason to construe *Smith* more broadly in the twenty-first century than the twentieth. Precise, persistent tracking reveals intimate details of a person's life,[480] and carrying a cell phone has, as Justice Kennedy put it, become essential to self-expression and even self-identity.[481] *Smith* should not apply to such data.

The third-party doctrine should not apply to cell phone location tracking of any kind, whether the information is voluntarily exposed or the result of a GPS ping. Courts should consider the acquisition of such data a search within the meaning of the Fourth Amendment.

B. Payton *Authorizes Limited Cell Phone Tracking to Aid Apprehension*

An arrest warrant will render some searches reasonable that would otherwise be unreasonable.[482] *Payton* grants police the authority to enter a house for the limited purpose of executing an arrest warrant.[483] *Bermudez* held that this power justifies the "lesser intrusion" of cell phone tracking.[484] Judge Gauvey disagreed, calling precise, persistent tracking a "different, and arguably more" intrusive search.[485]

Bermudez only considered the second type of search discussed in Part III.A.1, one that resembles the search in *Karo*.[486] *Bermudez* is correct: a single instance of tracking the subject into the home is less intrusive than a physical *Payton* entry. *Specified Wireless Telephone* primarily considered the first type of search: a mosaic of public and private movements that reveals intimate details of the subject's life.[487] Whether *Payton* justifies that search is a thornier question.

Judge Gauvey wrote that *Payton* could not justify this sort of mosaic search.[488] Because the government cited no authority applying *Payton* to location tracking, Judge Gauvey rejected the theory.[489] However, as Kerr explains, the application is novel because the concept of privacy in location and movement is itself novel.[490] Preexisting doctrines may apply to new legal concepts. While the novel application of *Payton* to tracking should be scrutinized, it cannot be dismissed out of hand. The *Payton* opinion

---

478. *See supra* Part I.B.5.
479. *See supra* Part I.B.5.b.
480. *See supra* notes 322–24 and accompanying text.
481. *See supra* note 209 and accompanying text.
482. *See supra* Part I.C.4.
483. *See supra* note 281 and accompanying text.
484. *See supra* Part II.B.1.b.
485. *See supra* note 336 and accompanying text.
486. In *Karo*, agents tracked a beeper from public roads into a private home. *See supra* Part II.B.1.
487. *See supra* notes 322–24 and accompanying text.
488. *See supra* notes 327–36 and accompanying text.
489. *See supra* notes 326–28 and accompanying text.
490. *See supra* notes 406–08 and accompanying text.

considered entry into a home the most intrusive of police actions.[491] To the extent precise, persistent tracking is a lesser intrusion, it should be permitted. However, this is the beginning of the argument, not the end.

Payton justifies a significant intrusion, but it does not justify information-gathering.[492] Judge Gauvey is correct in this regard.[493] Precise, persistent tracking may be less intrusive than a *Payton* search, but it can provide considerably more information.[494] *Payton* provides authority to cross the threshold of the home but no authority to investigate beyond what is necessary to locate the arrestee.[495] Police arresting inside the home can perform protective sweeps and search for accomplices to protect their own safety and to prevent the destruction of evidence, but such powers are not inherent to a *Payton* search.[496] Each power is designed for a particular hazard when police are inside a home and must be justified by specific facts.[497]

Those powers do not apply in the context of cell phone tracking, which presents none of the dangers of in-home arrests. A *Payton* search may reveal information in plain view, but police cannot investigate more than necessary to arrest the person. While an arrestee cannot forestall a justified protective sweep by cooperating with a *Payton* search of the home, cooperation could conceivably narrow the scope of the search by reducing the risk to officer safety or of the destruction of evidence.[498] In contrast, the subject has no knowledge of cell phone tracking, which allows police to search even when the suspect wishes to cooperate. Additionally, a *Payton* physical entry is a one-time event, which limits the information it can reveal.[499] Police could not rearrest the suspect later to find more incriminating evidence. Uncontrolled tracking, however, would tempt police into delaying arrest while learning the defendant's movements.

For precise, persistent tracking to be a reasonable search under *Payton*, it must be limited. Tracking used exclusively to facilitate arrest is reasonable. Any information police uncover during such a search would be analogous to objects within plain view during a *Payton* search.[500] Tracking for an investigative purpose, even ostensibly to execute an arrest warrant, is an unreasonable search, unjustified by *Payton* or any other doctrine. Both *Bermudez* and Judge Gauvey's opinion can peacefully coexist under this

491. *See* Payton v. New York, 445 U.S. 573, 585 (1980).
492. *See supra* notes 281–92 and accompanying text.
493. *See supra* notes 326–35 and accompanying text.
494. *See supra* notes 335–36 and accompanying text.
495. *See supra* notes 281–92 and accompanying text.
496. *See supra* notes 282–88 and accompanying text.
497. *See supra* notes 282–88 and accompanying text.
498. Because the doctrines discussed above often enable the police to investigate further, in an actual home arrest, a home would likely be subject to some investigation even if the arrestee cooperated at the door.
499. *Payton* does not explicitly prevent the police from repeatedly attempting to arrest a subject in his home, but repeat attempts are highly unlikely in practice. Presumably, police would either find the suspect at home or his absence would dispel the reasonable suspicion that he could be found there.
500. *See supra* notes 288–91 and accompanying text.

analysis. In *Bermudez*, police attempted to make the arrest within a day of beginning tracking.[501] That search was reasonable under *Payton*. Judge Gauvey rejected an application for thirty days of tracking.[502] If given access to the exact location of the person to be arrested, officers should be able to arrest him in a matter of hours, not weeks. Thirty days of precise, persistent tracking facilitates an investigation, not an arrest.

C. Cell Phone Tracking Must Be Tightly Controlled

The courts' challenge is to craft rules for tracking that facilitate arrest while protecting the rights of the arrestee. Tracking to facilitate arrest will only be necessary when the suspect's crime is unrelated to his location or movements.[503] Probable cause to arrest will often provide probable cause to track a suspect's movements, if movement and location will provide evidence of the crime.[504] Because tracking to facilitate arrest will only be necessary when location is *not* evidence of the crime leading to arrest, tight limitations are important. An arrest warrant should not justify a fishing expedition for evidence of a more serious crime.

Tracking the subject of an arrest warrant should only be allowed pursuant to a court order. While *Payton* allows police to enter the home of the subject of an arrest warrant without judicial approval,[505] the unique nature of precise, persistent tracking justifies this imposition. Neutral magistrates, not the officers themselves, are best positioned to ensure that police do not use tracking for investigative purposes.[506] Requiring court approval is also necessary to protect the Fourth Amendment rights of third parties, whose homes would be searched if they contained the tracked cell phone.

Court oversight also prevents police from having more power to track a suspect under an arrest warrant than under a search warrant.[507] Generally, orders allowing tracking to facilitate arrest should only sanction tracking for a few days or a reasonable time. A few days is likely ample time to effect most arrests.[508] If police have reason to believe that an arrest will take longer, or if they face unforeseen difficulties, a magistrate could grant more time. The paramount concern should be giving police only the time necessary to make the arrest.

This approach has one further advantage. If tracking is limited to the time necessary to make the arrest, it will not be a mosaic search at all. A few days will seldom reveal the sort of intimate details of the subject's life contemplated in *Maynard*.[509]

---

501. *See supra* note 351 and accompanying text.
502. *See supra* notes 310–11 and accompanying text.
503. *See supra* Part I.C.3.
504. *See supra* Part I.C.3.
505. *See supra* note 281 and accompanying text.
506. *See supra* notes 261–62 and accompanying text.
507. Search warrants for tracking are time-limited, but arrest warrants are not. *See supra* note 258 and accompanying text.
508. *See supra* notes 438–39 and accompanying text.
509. Precise tracking into the home for any period is still a search under *Karo*, but that search is more easily justified under *Payton*. *See supra* notes 486–87 and accompanying text.

Under this approach, because *Payton* authorizes tracking to facilitate arrest, the government need not meet the standards *Specified Wireless Telephone* sets forth for acquiring a search warrant to apprehend the suspect. The ability to track under an arrest warrant obviates the need for a separate search warrant to "look anywhere."[510] Moreover, careful judicial control of the tracking will mitigate potential abuse. Police can indeed look anywhere by tracking, but strict time-limiting prevents the sort of general investigative activity that troubled *Specified Wireless Telephone* and the framers of the Fourth Amendment.[511]

Requiring a court order serves a second, related purpose: drawing a bright line between the pre-arrest investigation and the performance of the arrest itself. An arrest warrant carries no time limit, so police can continue investigating the suspect long after securing an arrest warrant.[512] A traditional *Payton* home arrest necessarily ends the pre-arrest investigation phase, because the suspect is brought into custody. Agents making the arrest do not have a free hand to investigate during a *Payton* search, except under exigent circumstances.[513] And cell phone tracking does not involve the same exigencies—danger to the officers and destruction of the evidence—as in-home arrests. Precise, persistent tracking is an application of the *Payton* doctrine, and it should be subject to the same limitation. When police apply for a court order authorizing tracking, their pre-arrest investigation should be over. As if they had entered a house that presented no justification for a protective sweep,[514] they must try to make the arrest as soon as possible after beginning tracking. If police could track while they investigate, they could not avoid using tracking *to* investigate. The magistrate's order creates the appropriate separation.

In sum, requiring a court order and strict time-limiting ensures that precise, persistent tracking is used to facilitate arrest, not to further an investigation.

CONCLUSION

Precise cell phone tracking is a useful tool, allowing police to make arrests quickly and efficiently. Police should not be denied this ability, but it cannot become an investigative tool. While precise, persistent tracking of a cell phone is a search, it can be reasonable if used to facilitate arrest pursuant to an arrest warrant. Because *Payton* authorizes police entry into the home, it allows the lesser intrusion of cell phone tracking. However, police can only enter the home to perform an arrest, and tracking should be subjected to the same limitations. Judicial supervision ensures that tracking is used to help make the arrest, not to investigate the arrestee. If precise, persistent tracking is performed under court supervision and is only used to facilitate arrest, it is constitutional under the Fourth Amendment.

---

510. *See supra* notes 347–49 and accompanying text.
511. *See supra* notes 50–51 and accompanying text.
512. *See supra* notes 263–64 and accompanying text.
513. *See supra* Part I.C.4.
514. *See supra* notes 282–92 and accompanying text.