

4-1-2010

Warranting A Warrant: Fourth Amendment Concerns Raised By Law Enforcement's Warrantless Use Of GPS And Cellular Phone Tracking

Adam Koppel

Follow this and additional works at: <https://repository.law.miami.edu/umlr>



Part of the [Law Commons](#)

Recommended Citation

Adam Koppel, *Warranting A Warrant: Fourth Amendment Concerns Raised By Law Enforcement's Warrantless Use Of GPS And Cellular Phone Tracking*, 64 U. Miami L. Rev. 1061 (2010)
Available at: <https://repository.law.miami.edu/umlr/vol64/iss3/7>

This Note is brought to you for free and open access by the Journals at University of Miami School of Law Institutional Repository. It has been accepted for inclusion in University of Miami Law Review by an authorized editor of University of Miami School of Law Institutional Repository. For more information, please contact library@law.miami.edu.

NOTES

Warranting a Warrant: Fourth Amendment Concerns Raised by Law Enforcement's Warrantless Use of GPS and Cellular Phone Tracking

ADAM KOPPEL[†]

The Fourth Amendment does, of course, leave room for the employment of modern technology in criminal law enforcement, but . . . electronic monitoring, subject only to the self-restraint of law enforcement officials, has no place in our society.

—Justice John Harlan II*

I. INTRODUCTION	1062
II. TECHNOLOGICAL DEVELOPMENT OVERVIEW: THE TECHNOLOGICAL BASIS OF TRACKING AND POSSIBLE LAW ENFORCEMENT USES	1063
A. <i>GPS Tracking Devices</i>	1063
B. <i>Cellular Phone Site Location</i>	1066
III. THE SUPREME COURT'S FRAMEWORK OF FOURTH AMENDMENT ANALYSIS FOR EMERGING TECHNOLOGIES AND THE REASONABLE EXPECTATION OF PRIVACY DOCTRINE	1069
IV. THE CURRENT COURTS ARE SPLIT ON THE LEGALITY OF WARRANTLESS POLICE USE OF BOTH GPS DEVICES AND CELLULAR PHONE TRACKING	1072
A. <i>Some Courts Have Held that a Warrant Is Necessary for Police to Engage in GPS Tracking Due to the Intrusive Nature of this Technology that Goes Beyond Mere Sense-augmented Surveillance</i>	1073
B. <i>Some Courts Have Held that Warrantless GPS Tracking is Constitutional, as the Level of Intrusiveness Raises No Fourth Amendment Concerns</i>	1077
C. <i>The Statutory Debate over Governmental Access to Prospective, Real-time Cellular Phone Site Information</i>	1079
1. SOME COURTS HAVE HELD THAT A PROBABLE CAUSE SHOWING IS REQUIRED FOR LAW ENFORCEMENT TO OBTAIN CELLULAR LOCATION INFORMATION FROM SERVICE PROVIDERS	1080
2. SOME COURTS HAVE HELD THAT A BURDEN OF SPECIFIC AND ARTICULABLE FACTS IS REQUIRED FOR LAW ENFORCEMENT TO OBTAIN CELLULAR LOCATION INFORMATION FROM SERVICE PROVIDERS	1082
V. GPS TRACKING AND CELLULAR PHONE TRACKING SHOULD BE DEEMED A SEARCH WITHIN THE MEANING OF THE FOURTH AMENDMENT, REQUIRING POLICE TO OBTAIN A WARRANT BEFORE USE	1083
A. <i>GPS Tracking</i>	1083

[†] J.D. Candidate 2010, University of Miami School of Law; B.B.A. 2007, University of Miami. I would like to thank my family for their constant support in everything that I do.

* *United States v. White*, 401 U.S. 745, 790 (1971) (Harlan, J., dissenting).

B. <i>Cellular Phone Tracking</i>	1086
VI. CONCLUSION	1089

I. INTRODUCTION

Times have changed since telephones were hardwired to homes and people read maps to navigate their travels. Today, portable cellular phones dominate the communication world, and Global Positioning System, or GPS, technology guides users via satellite. These new technologies provide countless benefits to citizens and have greatly transformed our society. However, such conveniences do not come without a cost. While portable cell phones and GPS devices follow us around everywhere we go, these technologies also allow us to be followed everywhere we go.

Vehicle GPS tracking and cellular phone location tracking are new methods of surveillance, which use emerging forms of technology. These practices require judicial attention, as they can lead to major constitutional issues when law enforcement improperly uses them. Fourth Amendment privacy concerns arise when police use new methods of technology without a warrant and collect information in which an individual has a reasonable expectation of privacy. These two new technologies allow law enforcement to continuously track people by way of their cellular telephone or vehicle, usually without the user's knowledge. Advanced and powerful methods of surveillance can be overly intrusive by providing an abundance of information in real time about the private daily activities of every person.

Many people undervalue this type of tracking and do not see it as a great invasion of privacy. For instance, one might think it does not matter if the police are aware that he goes to lunch at a specific restaurant everyday or that he attends a certain church service every Sunday. However, this line of thinking misses a larger point. If someone has the ability to know the real-time location of a person around the clock, then one is able to create a full picture of that person's life. One learns everything about that person, much of which is highly personal and private in nature, going beyond what both the individual and society would consider a reasonable expectation of privacy.

This article explains why the Supreme Court needs to address the constitutional implications of warrantless law-enforcement surveillance methods of GPS tracking devices and cellular site location tracking. Part II discusses the history of both GPS devices and cellular telephones, describing the many uses for both citizens and law enforcement. Part III examines the framework of the Fourth Amendment analysis, outlining the Supreme Court's historical treatment of emerging technologies and

the reasonable expectation of privacy doctrine. Part IV discusses how the current courts are split as to the constitutionality of warrantless tracking by GPS devices and cellular telephone site location. Part V argues that, under the existing framework for analyzing enhanced surveillance, the Court should find that both of these technologies transmit information in which an individual has a reasonable expectation of privacy and, therefore, they should fall within the purview of the Fourth Amendment, requiring police to obtain a warrant prior to use.

II. TECHNOLOGICAL DEVELOPMENT OVERVIEW: THE TECHNOLOGICAL BASIS OF TRACKING AND POSSIBLE LAW-ENFORCEMENT USES

A. GPS Tracking Devices

The Global Positioning System is a satellite-based navigation system, which the U.S. Department of Defense developed in the early 1970s.¹ Today, GPS is also widely available to citizens, and the U.S. Air Force maintains it through a system that is accessible to both military and civilian users.²

GPS has three main components. First, a network of satellites orbits about 20,000 kilometers above the earth's surface and transmits ranging signals on two frequencies in the microwave part of the radio spectrum.³ The specific number of these satellites has consistently increased from the first full constellation of twenty-four satellites in 1994,⁴ up to the current network of thirty satellites, to ensure greater operability and accuracy of GPS.⁵ Second, a control segment maintains GPS through a system of ground-monitor stations and satellite-upload facilities.⁶ Third, user-receivers on Earth process the signals of at least four of these satellites, figure out the distance to each, and use this information to mathematically determine the receiver's location, velocity, and time.⁷ This process of determining a position from measurements of distances is known as trilateration (as opposed to triangulation, which involves the measurement of angles).⁸ Additionally, weather conditions do not affect GPS, allowing for continuous positioning and timing information

1. AHMED EL-RABBANY, *INTRODUCTION TO GPS: THE GLOBAL POSITIONING SYSTEM* 1 (2002).

2. Richard B. Langley, *In Simple Terms, How Does GPS Work?*, Mar. 24, 2003, <http://gge.unb.ca/Resources/HowDoesGPSWork.html>.

3. *Id.*

4. See SCOTT PACE ET AL., *THE GLOBAL POSITIONING SYSTEM: ASSESSING NATIONAL POLICIES* 246 (1995).

5. Langley, *supra* note 2.

6. *Id.*

7. See Marshall Brain & Tom Harris., *How GPS Receivers Work*, HOW STUFF WORKS, Sept. 25, 2006, <http://adventure.howstuffworks.com/gps.html>.

8. Langley, *supra* note 2.

twenty-four hours a day anywhere in the world.⁹

As GPS technology advances, receiver accuracy levels greatly increase as well. Currently, a basic receiver can accurately determine its position within a few meters.¹⁰ Further, by using a common process known as differential GPS, which incorporates additional correction signals to account for problems like atmospheric interference, a receiver can improve its positioning accuracy to within centimeters.¹¹

Over the past five years, there has been a vast increase in the popularity, availability, and affordability of GPS technology: "The Consumer Electronics Association estimates 20 percent of American households [currently] own a portable GPS system and 9 percent have vehicles equipped with in-dash systems."¹² Additionally, this increase is evident through the soaring end-of-year GPS sales estimates in the United States, generating over four-billion dollars in 2007.¹³ This increase in sales has been assisted by the drastic price decrease of GPS devices in the past three years. The average price of personal GPS devices has dropped almost fifty percent, from \$322 in 2006 to \$171 in 2007,¹⁴ and many units are now available for less than \$150.

In addition to drivers using GPS vehicle navigation systems to plot directions, GPS now has a variety of other uses, such as: allowing emergency services, including 911 or roadside assistance, to pinpoint the location of those in need of assistance; helping keep track of family members, either children or elderly members, so they do not wander off alone; easily finding lost pets using collars with built-in GPS; and allowing employers to keep tabs on employee hours or vehicle travel.¹⁵ GPS has even spread to the world of sports and can be used during a round of golf. A new waterproof, handheld GPS device uses the satellite-based GPS network and "calculates a golfer's distance to the center of the green or other features of the golf course, so he can select the proper club."¹⁶ GPS has uses in all areas of our lives, affecting and helping each of us in ways we may not even realize.

9. EL-RABBANY, *supra* note 1, at 1.

10. Langley, *supra* note 2.

11. PACE ET AL., *supra* note 4, app. A at 226.

12. Mitch Stacy, *Small GPS Devices Help Prosecutors Win Convictions*, ASSOCIATED PRESS, Aug. 30, 2008, available at <http://www.policeone.com/police technology/software/GIS/mapping/articles/1730192-Small-GPS-devices-help-prosecutors-winconvictions/>.

13. See *GPS Purchases to Generate \$4.1 Billion in Sales in 2007*, GPS WORLD, May 2007, http://findarticles.com/p/articles/mi_m0BPW/is_5_18/ai_n27257020/?tag=content;coll.

14. See Saul Hansell, *As Tech Buying Slows, G.P.S. Stays the Course*, N.Y. TIMES, Dec. 5, 2007, <http://bits.blogs.nytimes.com/2007/12/05/as-tech-buying-slows-gps-stays-the-course/>.

15. See Simon Wyrzowski, *12 Practical Uses of GPS for Everyday People*, EZINEARTICLES, Sept. 21, 2005, <http://ezinearticles.com/?12-Practical-Uses-of-GPS-for-Everyday-People&id=74085>.

16. See *GPS Comes to the Golf Course*, Posting of Brad Stone & Matt Richtel to N.Y. Times

In addition to the numerous benefits GPS has for consumers, this technology provides assistance in the field of law enforcement. GPS is applicable to a wide variety of law-enforcement problems and offers police substantial aid in each situation. For example, law-enforcement officials have used GPS in auto-theft sting operations¹⁷ and to monitor the whereabouts of parolees.¹⁸ Further, police have attempted to use records from suspects' personal, portable GPS devices as evidence of criminal activity. In Pennsylvania, "a trucker's GPS . . . led police to charge him with setting his own home on fire [after] GPS records showed his rig was parked about 100 yards from his house at the time of the fire."¹⁹

Most importantly, GPS receivers can be outfitted with wireless transmitters that send location information to third parties.²⁰ The third party can then remotely monitor the precise location of the GPS receiver from a tracking center.²¹ These features help law enforcement enhance covert-surveillance operations. Without a suspect's knowledge, police could approach a suspect's vehicle, magnetically attach a GPS tracking device to the vehicle's undercarriage, and view data from the device over a desktop or laptop computer.²² These systems are capable of lasting for weeks at a time, allowing police constant, real-time, and precise location information about that vehicle for much longer than they practically might be able to maintain round-the-clock visual surveillance.²³ This pervasive technology of remote suspect tailing is often conducted without a warrant, and, because the GPS devices used by law enforcement do not actually record conversations, they fall outside the scope of laws regulating wiretaps and similar forms of electronic surveillance.²⁴ To date, law-enforcement agencies have used these GPS features in

Bits Blog, <http://bits.blogs.nytimes.com/2009/01/08/gps-comes-to-the-golf-course/> (Jan. 8, 2009, 12:42 EST).

17. See *State v. Johnson*, No. 84282, 2005 WL 77090, at *1 (Ohio Ct. App. Jan. 13, 2005).

18. See *Chism v. State*, 813 N.E.2d 402, 406 (Ind. Ct. App. 2004), *vacated*, 824 N.E.2d 334 (Ind. 2005).

19. Stacy, *supra* note 12.

20. Renée McDonald Hutchins, *Tied Up In Knots? GPS Technology and the Fourth Amendment*, 55 UCLA L. REV. 409, 418 (2007).

21. *Id.*

22. See *State v. Jackson*, 76 P.3d 217, 221 (Wash. 2003) (en banc).

23. *Id.* at 223.

24. Dorothy J. Glancy, *Privacy on the Open Road*, 30 OHIO N.U. L. REV. 295, 315 (2004).

murder investigations,²⁵ robbery investigations,²⁶ drug investigations,²⁷ and public corruption cases.²⁸

Thus, it is clear that law enforcement may find GPS technology useful in a variety of contexts and for a variety of purposes. However, law enforcement's ability to use GPS to so scrupulously monitor individuals raises substantial Fourth Amendment concerns. As law enforcement's use of GPS has grown in recent years, so too have the challenges that defendants have raised, with most alleging Fourth Amendment violations due to warrantless use of GPS devices.

B. Cellular Phone Site Location

Today, there are more than 262 million cellular-phone subscribers in the United States.²⁹ Almost sixteen percent of United States households rely on wireless phones as their only source of telephone communication.³⁰

Wireless technology operates through a network of cell towers that emit radio frequencies capable of carrying calls, text messages, and other data.³¹ Cell towers are similar to traditional radio towers; however, they emit frequencies with much lower power, which allows many people in a small area to communicate over the same frequencies without interference.³² These cell towers are distributed throughout a coverage area and are usually much closer together in big cities with large numbers of users.³³ Additionally, cell phone users are often in range of more than one cell tower at a given time.³⁴

25. See *Jackson*, 76 P.3d at 221 (stating that detailed GPS information, including locations of the suspect's truck for exact periods of time, led to the discovery of a missing nine-year-old victim's body).

26. See *People v. Lacey*, No. 2463N/02, 2004 WL 1040676, *1-2 (N.Y. Crim. Ct. May 6, 2004) (showing police used information from a placed GPS tracker as evidence of a robbery suspect's location near several robberies), *aff'd*, 887 N.Y.S.2d 158 (App. Div. 2009).

27. See *United States v. McIver*, 186 F.3d 1119, 1123 (9th Cir. 1999) (describing how police placed a GPS tracker on a drug suspect's vehicle and used it to track the suspect on trips to a marijuana field).

28. Brandon Bain, 'Big Brother' Is Boss; Workers Object to Babylon's Satellite Tracking System, *NEWSDAY* (Long Island, N.Y.), Mar. 13, 2006, at A06 (describing how the police department in Clinton Township, New Jersey, installed GPS devices on several department patrol cars as part of an internal investigation of its own officers).

29. CTIA—THE WIRELESS ASS'N, CTIA'S SEMI-ANNUAL WIRELESS INDUSTRY SURVEY (2008), http://files.ctia.org/pdf/CTIA_Survey_Mid_Year_2008_Graphics.pdf.

30. Ryan Randazzo, *Quest Seeks Exemption on Rates*, *ARIZ. REPUBLIC*, July 11, 2008, at 1.

31. See Marshall Brain, Jeff Tyson & Julia Layton, *How Cell Phones Work*, *HOW STUFF WORKS*, Nov. 10, 2000, <http://www.howstuffworks.com/cell-phone.htm>.

32. See *id.*

33. See Posting of Tom Farley & Mark van der Hoeck to Privateline, http://www.privateline.com/mt_cellbasics (Jan. 1, 2006, 23:07 EST).

34. See Brain et al., *supra* note 31.

A significant characteristic of cellular phones is that they constantly relay their locations to cellular towers in order to have the strongest possible signal and to allow the next inbound call to be received without a delay.³⁵ This process, called registration, occurs every seven seconds, without the user of the phone needing to take any action, and the user is usually unaware that these signals are even being sent.³⁶ The information that service providers transmit and store, often called cell-site information, includes the subscriber's ten-digit phone number and a thirty-two-digit phone-identification number.³⁷ The only way for a user to stop these signals is to turn the phone off.³⁸

During phone calls, cellular systems are managed by mobile telephone switching offices that locate users based on tower signals and send incoming calls to their phones through the nearest tower.³⁹ As a user's location moves toward a closer tower during a call, the tower being used will switch through Time Difference of Arrival (TDOA) or Angle of Arrival (AOA) methods, measuring the strength of signal and thus the location of the cell phone.⁴⁰ To calculate the approximate location, TDOA measures the amount of time it takes a signal to travel from the phone to the tower, while AOA measures the angle at which the tower receives the phone's signal.⁴¹ The accuracy of location tracking depends on the geographic region, as the more densely placed the phone towers, the more accurate the location data will be. In urban areas with many towers, this location information can be within the range of a couple hundred feet, while in rural areas with fewer towers, the information can be within a few miles.⁴²

Though these features only reveal the general location of the user, other variations of wireless phone tracking permit location of the user with much greater accuracy. "Facing" is one feature that allows for a more accurate location range. Cell towers contain three sets of 120-degree panels, and the location of a user's phone can be found by deter-

35. Farley & van der Hoek, *supra* note 33.

36. *Id.*

37. *See id.*

38. *Id.* The purpose of this registration information is also based on billing rates for the cell phone service provider. *See id.* These signals allow providers to know the location of the phone and whether the phone is roaming, in order to apply the proper billing charges for these calls. *See id.*

39. *See* Brain et al., *supra* note 31.

40. Kevin McLaughlin, Note, *The Fourth Amendment and Cell Phone Location Tracking: Where Are We?* 29 HASTINGS COMM. & ENT. L.J. 421, 426 (2007); *see also* Brain et al., *supra* note 31.

41. McLaughlin, *supra* note 40, at 426.

42. *See In re Applications of U.S. for Orders Pursuant to Title 18, U.S. Code, Section 2703(d)*, 509 F. Supp. 2d 76, 78 n.3 (D. Mass. 2007).

mining which of these panels is communicating with the user's phone.⁴³ An even more precise method of location occurs through a process called "triangulation," which uses AOA or TDOA to calculate the relative signal strength of the three nearest cellular towers.⁴⁴

The ability for such accurate location tracking has socially beneficial applications, most notably the ability to pinpoint the location of 911 emergency calls made from cellular phones.⁴⁵ Other daily examples of this technology include keeping track of family members, especially children or spouses, and employers using the technology in businesses to log the location of mobile employees.⁴⁶

Just as cellular phone tracking is desired by civilians, this powerful and advanced method of surveillance has also been highly sought after by law-enforcement agencies. Law-enforcement officials are especially interested in this information because they can use it to determine a suspect's approximate location and to track his or her movements.⁴⁷ The major issue with this is that cell phone companies usually own the cell towers, and these companies are in control of the relevant information.⁴⁸ This type of electronic surveillance is generally governed by the Electronic Communications Privacy Act of 1986 (ECPA).⁴⁹ Pursuant to the requirements of the ECPA, for law enforcement to obtain location tracking information, they must seek a court order requiring the cellular service provider to turn over this data.⁵⁰ The current debate is centered on the legal standard required for obtaining these orders. Some courts indicate that the government only has the burden of proving specific and articulable facts, and sometimes even less, for these orders. However, other courts require the government to provide a showing of probable cause to obtain the orders.⁵¹

Finally, the type of tracking information sought by law enforcement is an issue affecting this controversy. Police may request that a service provider turn over the stored records of cell location data to reconstruct a picture of where a suspect was located at a given time in the past.⁵² This

43. See McLaughlin, *supra* note 40, at 427; Farley & van der Hoek, *supra* note 33.

44. McLaughlin, *supra* note 40, at 427.

45. See David Colker, *Go Ahead, Just Try to Disappear; Global Positioning Technology on Mobile Phones and Other Devices Can Track Errant Workers, Teens or Even Pets*, L.A. TIMES, Dec. 27, 2004, at A1.

46. See *id.*

47. See *United States v. Forest*, 355 F.3d 942, 947 (6th Cir. 2004), *vacated sub nom. Garner v. United States*, 543 U.S. 1100 (2005).

48. See Ian James Samuel, Note, *Warrantless Location Tracking*, 83 N.Y.U. L. REV. 1324, 1327-28 (2008).

49. 18 U.S.C. §§ 2510-2522 (2006).

50. *Id.* § 2516.

51. See *infra* notes 157-73 and accompanying text.

52. See, e.g., *In re Application of the U.S. for an Order Authorizing the Installation & Use of*

information, called “historical data,” is limited in value and usually produces a lower level of concern from privacy advocates.⁵³ Alternately, law enforcement may seek real-time tracking information about individuals.⁵⁴ When this type of information is sought, law enforcement must ask the court for a prospective order because such real-time data is inherently not yet in existence at the time of the request.⁵⁵

In light of the vast increase in mobile technology and the large debate within the courts on the topic, there is a strong need for Fourth Amendment guidance in this area. Similar to the recent law-enforcement use of GPS tracking devices, use of this cellular phone tracking information raises numerous privacy issues. This powerful investigative tool can reveal sensitive information and can be overly intrusive if used without a warrant. Moreover, as most Americans voluntarily carry cell phones, cell phone tracking is different from the surveillance technology of the past.

III. THE SUPREME COURT’S FRAMEWORK OF FOURTH AMENDMENT ANALYSIS FOR EMERGING TECHNOLOGIES AND THE REASONABLE EXPECTATION OF PRIVACY DOCTRINE

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.⁵⁶

The courts will find a search unreasonable, and therefore unconstitutional, if it is conducted without a warrant, unless “exceptional circumstances” are shown.⁵⁷ For the warrant protections of the Fourth Amendment to become relevant, the use of these emerging technologies by law enforcement must be deemed a search.⁵⁸ If no search occurred, the Fourth Amendment does not apply.

Historically, the inquiry over whether a search took place under the Fourth Amendment focused on if a physical trespass had occurred.⁵⁹ The

a Pen Register & a Caller Identification Sys. on Tel. Nos. [Sealed] & [Sealed] & the Prod. of Real Time Cell Site Info., 402 F. Supp. 2d 597, 599 (D. Md. 2005) [hereinafter *Maryland*].

53. McLaughlin, *supra* note 40, at 432.

54. *See Maryland*, 402 F. Supp. 2d at 599.

55. *Id.*

56. U.S. CONST. amend. IV.

57. *Johnson v. United States*, 333 U.S. 10, 13–15 (1948).

58. *See, e.g., Kyllo v. United States*, 533 U.S. 27, 31 (2001); *Dow Chem. Co. v. United States*, 476 U.S. 227, 239 (1986) (“[T]he taking of aerial photographs . . . is not a search prohibited by the Fourth Amendment.”).

59. *Kyllo*, 533 U.S. at 31; *see, e.g., Olmstead v. United States*, 277 U.S. 438, 463 (1928)

Supreme Court altered this line of thinking in the seminal case *Katz v. United States*.⁶⁰ The Court held for the first time that "the Fourth Amendment protects people, not places,"⁶¹ and that the Fourth Amendment's purpose is to protect individuals' reasonable expectation of privacy from government intrusion.⁶² The context of the *Katz* decision indicates that the Court was attentive to the effects of emerging technology and factored in the ability of police to obtain information without any physical intrusion.⁶³

The Supreme Court from then on adopted Justice Harlan's two-pronged formulation of Fourth Amendment application as the standard analysis for determining whether or not a search has occurred. Under this method there are two requirements necessary to find that a person had a reasonable expectation of privacy. The inquiry is as follows: "[F]irst, that a person have exhibited an actual (subjective) expectation of privacy, and, second, that the expectation be one that society is prepared to recognize as 'reasonable.'"⁶⁴ Using this formula, the Court uses intrusiveness to measure objective reasonableness. The question of whether a search occurred has become a matter of case-by-case, technology-by-technology analysis.

We can further learn how the Court treats emerging technologies by examining the line of post-*Katz* surveillance cases. These cases dealt with the warrantless use of new forms of surveillance in which the Court's focus was the specific type of technology used and the level of information it revealed. In *United States v. Caceres*,⁶⁵ the Court faced the issue of whether the Fourth Amendment prohibited use of a recording device during conversations with the defendant.⁶⁶ The Court held that it did not and declined to define the use of the device as search.⁶⁷ The Court reasoned that the information received from the recording device was merely equivalent to an agent taking written notes; so no invasion of the defendant's expectation of privacy had occurred.⁶⁸

In the same year, the Court considered the warrantless use of a pen

(describing how a Fourth Amendment violation depended on whether officers penetrated the defendants' home), *overruled by* *Katz v. United States*, 389 U.S. 347 (1967), *and* *Berger v. New York*, 388 U.S. 41 (1967).

60. 389 U.S. 347 (1967).

61. *Id.* at 351.

62. *Id.* at 351-53.

63. *See id.* at 352-53.

64. *Id.* at 361 (Harlan, J., concurring).

65. 440 U.S. 741 (1979).

66. *Id.* at 743.

67. *Id.* at 744.

68. *See id.* at 751.

register by law enforcement.⁶⁹ In *Smith v. Maryland*, the Court held that no search had occurred from use of the pen register and allowed warrantless use of the technology.⁷⁰ The Court explained that in dialing a phone number, the user is voluntarily conveying the number to the phone company and thus assumes the risk that this information may be passed on to the police.⁷¹ Further, the Court characterized a pen register as a sense-augmenting device because it discloses only the number that has been dialed; it does not reveal any other information about the caller or recipient.⁷²

The next category of surveillance technology that the Court addressed was a battery-operated beeper that acts as a tracking device by emitting a weak radio signal, which can be followed by a nearby agent with a receiver.⁷³ The Court analyzed the warrantless use of these electronic beepers in *United States v. Knotts* and *United States v. Karo*.

In *Knotts*, law-enforcement officers obtained consent from a chemical manufacturing company to install a tracking beeper inside a container of chloroform, and then tracked defendant's movements when he later transported the container.⁷⁴ The Court classified this type of device as merely sense augmenting, because normal visual surveillance alone would also have allowed the police to view the movements of the container.⁷⁵ The Court found there was no violation of any reasonable expectation of privacy when the beeper was used to simply follow the movements of the individuals in plain view on public thoroughfares.⁷⁶ Thus, the Court found that use of the beeper did not amount to a search, and no Fourth Amendment violation occurred.⁷⁷

In contrast, the Court in *Karo* held that warrantless use of an electronic tracking beeper constituted a search and violated the Fourth Amendment when law enforcement used the beeper to establish its location inside a private home.⁷⁸ The Court acknowledged the limited nature of information available through beeper technology, but focused on the

69. See *Smith v. Maryland*, 442 U.S. 735, 736 (1979). "A pen register is a mechanical device that records the numbers dialed on a telephone by monitoring the electrical impulses caused when the dial on the telephone is released." *Id.* n.1 (internal quotation marks omitted).

70. *Id.* at 745–46.

71. *Id.* at 744–45. The assumption of risk analysis stemmed from the line of cases starting with *United States v. Miller*, 425 U.S. 435, 443 (1976), holding that a person has no expectation of privacy in financial information voluntarily exchanged to a bank.

72. *Smith*, 442 U.S. at 741.

73. See *United States v. Knotts*, 460 U.S. 276, 277 (1983); see also *United States v. Karo*, 468 U.S. 705 (1984).

74. *Knotts*, 460 U.S. at 278.

75. *Id.* at 285.

76. *Id.* at 281.

77. *Id.* at 284–85.

78. *Karo*, 468 U.S. at 718.

fact that the beeper revealed information about the inside of the home that could not have been otherwise obtained without a warrant.⁷⁹ The Court recognized that society has an objectively reasonable expectation of privacy within the home.⁸⁰

Most recently, the Court extended its analysis of electronic surveillance to thermal imaging devices.⁸¹ In *Kyllo v. United States*, federal agents suspected that the defendant was growing marijuana in his home, so they used a thermal-imaging device to determine that a relatively high level of heat was radiating from the defendant's home and used this information to secure a search warrant.⁸² The Court found that the thermal imager was used as an extrasensory device because it revealed information regarding the interior of the home, and because the information was virtually unavailable to the average person.⁸³ The Court held that use of the technology constituted a search under the Fourth Amendment and was unconstitutional without a warrant.⁸⁴

The Supreme Court's framework of analysis for emerging surveillance technologies provides some indication of how it may handle an inevitable challenge to GPS tracking or cell phone site tracking. The key inquiry is how the Court will characterize the technology and whether it believes an individual has a reasonable expectation of privacy in the information being revealed.

IV. THE CURRENT COURTS ARE SPLIT ON THE LEGALITY OF WARRANTLESS POLICE USE OF BOTH GPS DEVICES AND CELLULAR PHONE TRACKING

The Supreme Court has not yet addressed the emerging use of both GPS and cellular telephone site tracking by law enforcement. This issue is not premature and must be dealt with, as significant confusion exists among the lower courts and states on the legality of obtaining information via these techniques without a warrant. Courts have been divided mainly on the application of the reasonable expectation of privacy test to these new technologies. Additional challenges are inevitable, especially as the technology becomes more affordable and widely used by smaller police departments and the public alike. State and federal courts will be increasingly called upon to strike the proper balance between legitimate law enforcement objectives and maintenance of constitutional guaran-

79. *Id.* at 715.

80. *Id.* at 714.

81. *See Kyllo v. United States*, 533 U.S. 27 (2001).

82. *Id.* at 30.

83. *Id.* at 37-38.

84. *Id.* at 40.

tees in light of technological advances. These disagreements indicate that the Supreme Court will likely need to decide a case on both GPS use and cellular phone tracking in the near future.

A. Some Courts Have Held that a Warrant Is Necessary for Police to Engage in GPS Tracking Due to the Intrusive Nature of this Technology that Goes Beyond Mere Sense-augmented Surveillance

To date, four state courts have concluded (or assumed) that the use of a GPS device requires some form of prior judicial authorization. Two of these courts held that law enforcement violate their respective state constitutions when they place GPS tracking devices on vehicles without a warrant.⁸⁵ The third court assumed “without deciding, that the GPS surveillance of defendant’s vehicle was a search within the meaning of the Fourth Amendment”⁸⁶ The fourth state court held that probable cause is required for installation of a GPS tracking device, without ruling on the necessity of a warrant.⁸⁷

The most prominent GPS tracking case to recognize the constitutional implications of the technology is *State v. Jackson*, in which the Supreme Court of Washington became the first state court to deal with the question of whether a warrant is required for law enforcement to use GPS tracking of a criminal suspect.⁸⁸ In *Jackson*, police suspected that the defendant, William Bradley Jackson, had murdered his nine-year old daughter, and, based on that belief, the police obtained a warrant to impound and search two vehicles belonging to the defendant.⁸⁹ Without Jackson’s knowledge, police obtained a second warrant for the installation of GPS tracking devices on the impounded vehicles and returned the cars to Jackson without informing him the devices had been put in.⁹⁰ For nearly a month the police monitored the devices, logging Jackson’s location information and the time he spent at each site.⁹¹ The GPS devices eventually led the police to the location where Jackson had dumped the daughter’s body, and Jackson was later convicted of murder following a jury trial.⁹²

85. *People v. Lacey*, No. 2463N/02, 2004 WL 1040676, at *8 (N.Y. Crim. Ct. May 6, 2004) (finding that a warrant is required to install a GPS tracking device on a vehicle), *aff’d*, 887 N.Y.S.2d 158 (App. Div. 2009); *State v. Jackson*, 76 P.3d 217, 224 (Wash. 2003) (en banc) (finding that a warrant must be obtained prior to installation and use of a GPS device).

86. *People v. Obujen*, No. H026715, 2005 WL 519233, at *10 (Cal. Ct. App. Mar. 7, 2005).

87. *See State v. Scott*, No. 02-02-00121-I, 2006 WL 2640221, at *5 (N.J. Super. Ct. App. Div. Sept. 15, 2006) (per curiam).

88. *Hutchins*, *supra* note 20, at 447.

89. *Jackson*, 76 P.3d at 220–21.

90. *Id.*

91. *Id.*

92. *Id.* at 221.

On appeal, the intermediate appellate court rejected Jackson's challenge to the police use of the GPS device, finding that a warrant was not required to install and monitor the device.⁹³ However, the Supreme Court of Washington disagreed with the intermediate appellate court's conclusion. The Supreme Court of Washington held that the installation of a GPS tracking device constituted a search or a seizure under the Washington constitution, which provides that "[n]o person shall be disturbed in his private affairs, or his home invaded, without authority of law."⁹⁴ In holding that a warrant is required, the court did note that the Washington state constitution is more protective than the Fourth Amendment of the U.S. Constitution.⁹⁵ While the court found that GPS tracking by the government requires a warrant, it did not hold for the defendant. The court held that there was no constitutional violation because the police in this case had obtained valid warrants.⁹⁶

Though the *Jackson* court did not rely upon the Supreme Court's Fourth Amendment case law, its focus on the potential intrusiveness of the technology was entirely consistent with the directive of the *Katz* line of cases.⁹⁷ The court reasoned that GPS was a "particularly intrusive" method of surveillance because it did not merely augment a police officer's senses, such as when using binoculars or a flashlight; rather, it served as a total technological substitute for visual tracking because the officer does not actually follow the vehicle once the GPS device is attached.⁹⁸ The court further distinguished this technology from simply following a suspect on public roads, pointing out that police obtained this uninterrupted GPS information twenty-four hours a day for almost three full weeks, a time period very unlikely for a police officer to conduct standard visual surveillance.⁹⁹

Most importantly, the court was greatly concerned with the extensive level of personal detail a GPS tracking device provided law enforcement agents:

Moreover, the intrusion into private affairs made possible with a GPS device is quite extensive as the information obtained can disclose a great deal about an individual's life. For example, the device can provide a detailed record of travel to doctors' offices, banks, gambling casinos, tanning salons, places of worship, political party meetings, bars, grocery stores, exercise gyms, places where children are

93. *Id.* at 222.

94. *Id.* (alteration in original) (quoting WASH. CONST. art. 1, § 7) (internal quotation marks omitted).

95. *Id.*

96. *Id.* at 231.

97. Hutchins, *supra* note 20, at 448.

98. *Jackson*, 76 P.3d at 222-24.

99. *Id.* at 223.

dropped off for school, play, or day care, the upper scale restaurant and the fast food restaurant, the strip club, the opera, the baseball game, the “wrong” side of town, the family planning clinic, the labor rally. In this age, vehicles are used to take people to a vast number of places that can reveal preferences, alignments, associations, personal ails and foibles. The GPS tracking devices record all of these travels, and thus can provide a detailed picture of one’s life.¹⁰⁰

Given this invasion into private lives and allowance of intimate detail, the court held a warrant necessary to protect citizens’ rights to be free from government intrusion.¹⁰¹

The year after *Jackson*, a New York court addressed a case where police placed a GPS tracking device on the undercarriage of a burglary suspect’s vehicle. The court here in *People v. Lacey* also held that the installation and monitoring of a GPS tracking device without a warrant violated the New York version of the federal Fourth Amendment.¹⁰² Like in *Jackson*, the court focused on the intrusiveness and invasive nature of the technology, reasoning that “individuals must be given the constitutional protections necessary to their continued unfettered freedom from a ‘big brother’ society.”¹⁰³ The court acknowledged the diminished expectation of privacy that citizens have in their vehicles on public roads, however, merely parking a vehicle on a public street does not give law enforcement the right to surreptitiously attach a tracking device without a warrant or the owner’s consent.¹⁰⁴ “Other than in the most exigent circumstances, a person must feel secure that his or her every movement will not be tracked except upon a warrant based on probable cause establishing that such a person has been or is about to commit a crime.”¹⁰⁵ The *Lacey* court appreciated the importance of technological advances but realized the larger detriment to society if this technology abrogated our constitutional protections.¹⁰⁶

Though most case law specific to the warrant requirement for use of GPS lies in state courts, one federal court has also implied that GPS tracking devices may fall outside the *Knotts* precedent and require a warrant, however, found it unnecessary to resolve that question in its ruling.¹⁰⁷ In *United States v. Berry*, police obtained a court order from a Baltimore County circuit court to install a GPS tracking device to a sus-

100. *Id.*

101. *Id.* at 224.

102. *People v. Lacey*, No. 2463N/02, 2004 WL 1040676, at *8 (N.Y. Crim. Ct. May 6, 2004), *aff’d*, 887 N.Y.S.2d 158 (App. Div. 2009).

103. *Id.* at *7.

104. *Id.* at *8.

105. *Id.* at *7.

106. *Id.*

107. *See United States v. Berry*, 300 F. Supp. 2d 366, 368 (D. Md. 2004).

pect's vehicle.¹⁰⁸ Police then used information they received from the device to obtain a search warrant that led to a finding of narcotics.¹⁰⁹

The federal court did not need to decide whether GPS devices require a court order because they denied the defendant's suppression motion, relying upon the valid state-court search warrant.¹¹⁰ Nonetheless, the court did discuss that GPS devices may be more sophisticated than a beeper and fall outside the beeper precedents. The court distinguished modern GPS devices, which can serve as a complete substitute for police surveillance, from beepers, which merely augment visual surveillance.¹¹¹ Moreover, the court suggested that due to the advancement in GPS technology and the substantial amount of information available through the devices, the Supreme Court might find GPS "so intrusive that the police must obtain a court order before using it."¹¹²

The main line of reasoning from these cases is that even though GPS devices are considered a type of location-tracking device, they are distinguishable from previous tracking devices dealt with by courts, such as beepers. Beepers require actual and contemporaneous police surveillance as they function by merely telling police how close they are to the target vehicle, based on signal strength.¹¹³ In contrast, GPS devices do not require police presence in the area to provide data and give the target's exact coordinates without any additional visual surveillance.¹¹⁴ By monitoring through a computer, police can continuously track the target vehicle as a substitute for actual surveillance in person.¹¹⁵ Further, GPS devices are much more intrusive due to their accurate targeting (to within feet of the target) and their ability to last for lengthy periods of time.¹¹⁶ As recognized by the *Knotts* Court, these characteristics of GPS devices as a whole may equal the "dragnet-type" twenty-four hour surveillance that goes beyond the reach of the federal constitution.¹¹⁷

Thus, the main inquiry is whether GPS tracking devices provide information that intrudes upon an individual's reasonable expectation of privacy. These cases show that courts have clearly found both that it is

108. *Id.* at 367.

109. *Id.*

110. *Id.* at 368.

111. *Id.*

112. *Id.*

113. *State v. Scott*, No. 02-02-00121-I, 2006 WL 2640221, at *5 (N.J. Super. Ct. App. Div. Sept. 15, 2006).

114. *State v. Jackson*, 76 P.3d 217, 223 (Wash. 2003) (en banc).

115. *Scott*, 2006 WL 2640221, at *6.

116. *See, e.g., Jackson*, 76 P.3d at 223-24; *PACE ET AL.*, *supra* note 4, app. A. at 227.

117. *United States v. Knotts*, 460 U.S. 276, 284 (1983) ("[I]f such dragnet-type law enforcement practices as respondent envisions should eventually occur, there will be time enough then to determine whether different constitutional principles may be applicable.").

an invasion of reasonably expected privacy for the government to track locations with GPS and that a warrant is necessary to protect the public's right to privacy under these circumstances.

B. *Some Courts Have Held that Warrantless GPS Tracking is Constitutional, as the Level of Intrusiveness Raises No Fourth Amendment Concerns*

To date, two federal courts and one state court have explicitly found that law enforcement's surreptitious use of GPS devices against suspects did not raise any Fourth Amendment concerns. In the first of these cases, *United States v. Moran*,¹¹⁸ narcotics agents installed a GPS tracking device on the defendant's car, without first obtaining a warrant, and monitored its movement for the next two days.¹¹⁹ Prior to trial, the defendant moved to suppress any evidence obtained through the warrantless use of the device.¹²⁰ The court denied the motion and held there was no Fourth Amendment violation.¹²¹ In support of this holding, the *Moran* court relied solely on *Knotts* dicta that the defendant had no reasonable expectation of privacy while traveling on public thoroughfares.¹²² The court failed to offer any further reasoning or analysis outside of simply citing this authority and criticizing the New York court in *Lacey* for not considering *Knotts* in its decision.¹²³ Additionally, the *Moran* court did not address or consider any differences between the beeper used in *Knotts* and the much more advanced and intrusive GPS device at issue in *Moran*. The court merely treated use of the GPS device as indistinguishable from mere visual surveillance.¹²⁴

After *Moran*, in *People v. Gant*, the Westchester County Court of New York also refused to recognize any Fourth Amendment concerns by law enforcement's use of a GPS tracking device.¹²⁵ The *Gant* court addressed a defendant's challenge to police officers' warrantless attachment and use of a GPS device that was placed on the defendant's recreational vehicle.¹²⁶ Following *Knotts* and *Moran*, the court reasoned that a person traveling on public thoroughfares has no legitimate expectation of privacy in his movements from one place to another.¹²⁷ With the

118. 349 F. Supp. 2d 425 (N.D.N.Y. 2005).

119. *Id.* at 467.

120. *Id.*

121. *Id.* at 468.

122. *Id.* at 467 (citing *Knotts*, 460 U.S. at 281).

123. *See id.* (citing *People v. Lacey*, No. 236N/02, 2004 WL 1040676, at *8 (N.Y. Crim. Ct. May 6, 2004)).

124. *See id.*

125. 802 N.Y.S.2d 839 (N.Y. Crim. Ct. 2005).

126. *Id.* at 845.

127. *See id.* at 847.

defendant having no reasonable expectation of privacy, the court held that no search or seizure occurred and there were no Fourth Amendment implications from use of the device.¹²⁸ Like in *Moran*, the court relied on *Knotts*, but failed to address the intrusive capabilities of modern GPS devices. The court merely assumed that this new technology is analogous to beeper technology without discussing the clear differences.¹²⁹

The most recent GPS case in which a court rejected the warrant requirement came from Judge Posner of the Seventh Circuit in *United States v. Garcia*.¹³⁰ In *Garcia*, police, without a warrant, placed a GPS “memory tracking unit” underneath the bumper of defendant’s car when it was parked on a public street.¹³¹ This device “receive[d] and store[d] satellite signals that indicate[d] the device’s location. So when the police later retrieved the device . . . they were able to learn the car’s travel history since the installation of the device.”¹³² The information gained from the device eventually led to a finding of defendant’s participation in crimes relating to the manufacturing of methamphetamine.¹³³ Defendant moved to suppress evidence obtained as a result of the tracking device as the fruit of an unconstitutional search.¹³⁴

Posner rejected defendant’s challenge and thoroughly criticized a warrant requirement for GPS devices.¹³⁵ Posner first found it untenable that attachment of the GPS tracking device constituted a seizure, as no meaningful interference occurred with the defendant’s possession of the vehicle.¹³⁶ Next, Posner established that the police activity did not amount to a search either.¹³⁷ Posner asserted that GPS tracking is equivalent to the use of beeper technology present in *Knotts*, and therefore should not be considered a search.¹³⁸ Posner did recognize the vast amount of information that may be gathered through warrantless GPS tracking and also addressed that the Fourth Amendment must move ahead as technology advances.¹³⁹ However, Posner cautioned that greater security often comes at the cost of privacy, and, thus, no warrant

128. *Id.*

129. *See id.* at 846–47.

130. 474 F.3d 994 (7th Cir. 2007).

131. *Id.* at 995.

132. *Id.*

133. *Id.*

134. *Id.*

135. *Id.* at 996–98.

136. *Id.* at 996 (“The device did not affect the car’s driving qualities, did not draw power from the car’s engine or battery, did not take up room that might otherwise have been occupied by passengers or packages, did not even alter the car’s appearance, and in short did not ‘seize’ the car in any intelligible sense of the word.”).

137. *Id.* at 997.

138. *Id.* at 998.

139. *Id.*

is necessary for this activity.¹⁴⁰

On the whole, the courts in this line of cases mainly reach their conclusions by evading the question of whether such tracking constitutes a more substantial intrusion on privacy than previously considered forms of surveillance. The courts have equated GPS technology with beeper surveillance of the past without any reasoning or analysis of the comparisons between the two. Moreover, a major issue revolves around what specific type of GPS tracking device is being used by police. For example, in *Garcia*, the GPS device was a memory-tracking unit that simply received and stored satellite signals, which indicated the device's location.¹⁴¹ In order for police to obtain any desired information, they had to physically go and retrieve the device to learn the car's travel history.¹⁴² This type of device differs greatly from GPS devices that transmit location information in real time over the computer. When faced with a case involving real-time GPS tracking by police, courts may recognize that more protection is required due to the larger risk of intrusion.¹⁴³

C. *The Statutory Debate over Governmental Access to Prospective, Real-time Cellular Phone Site Information*

The Electronic Communications Privacy Act (ECPA) of 1986 is currently the most influential legislation governing electronic surveillance issues. Congress intended Title I of the ECPA to address the interception of wire, electronic, and oral communications.¹⁴⁴ Congress created Title II to deal with government access to "stored wire and electronic communications and transactional records."¹⁴⁵ Title III addresses "pen registers and trap and trace devices."¹⁴⁶ These three titles within the ECPA have been interpreted as setting out four separate categories of legal requirements for governmental officials to receive judicial authorization to obtain various types of cell site information from third-party service providers: super warrants, probable cause, specific and articulable facts, and a lower standard of mere relevancy.¹⁴⁷

First, Title I provides the greatest level of protection for cellular

140. *See id.*

141. *Id.* at 995.

142. *Id.*

143. *See, e.g.,* *People v. Obujen*, No. H026715, 2005 WL 519233, at *10 (Cal. Ct. App. May 7, 2005); *State v. Scott*, No. 02-02-00121-1, 2006 WL 2640221, at *5 (N.J. Super. Ct. App. Div. Sept. 15, 2006); *People v. Lacey*, No. 2463N/02, 2004 WL 1040676, at *8 (N.Y. Crim. Ct. 2004), *aff'd*, 887 N.Y.S.2d 158 (App. Div. 2009); *State v. Jackson*, 76 P.3d 217, 223 (Wash. 2003).

144. S. REP. NO. 99-541, at 3 (1986), *reprinted in* 1986 U.S.C.C.A.N. 3555, 3556.

145. *Id.*

146. *Id.*

147. Rickey G. Glover, Note, *A Probable Nightmare: Lifting the Fog from the Cellular Surveillance Statutory Catastrophe*, 41 VAL. U. L. REV. 1543, 1558 (2007).

communications, forcing the government to meet super warrant requirements before intercepting phone conversation content.¹⁴⁸ Second, the government's burden for obtaining customer records concerning electronic communication service or remote computing service, discussed in Title II of the ECPA, is a showing of specific and articulable facts regarding the government's need for the information.¹⁴⁹ Third, the authority required for governmental use of tracking devices is a showing of probable cause pursuant to Federal Rule of Criminal Procedure 41.¹⁵⁰ Fourth, to obtain information from a pen register or trap and trace device, the government must simply demonstrate the material is relevant to an ongoing criminal investigation.¹⁵¹

The current debate centers around the appropriate legal standard required for obtaining prospective, real-time cell site information from third-party cellular service providers. This standard depends on what aspect of the ECPA the court believes is implicated. Recent cases on the topic have begun to establish the general consensus that the government cannot obtain cell tower site location information solely under the pen register statute.¹⁵² Thus, the main division amongst courts is whether the data should be treated like a tracking device, requiring probable cause, or whether the data should be treated as subscriber records, requiring specific and articulable facts.

1. SOME COURTS HAVE HELD THAT A PROBABLE CAUSE SHOWING IS
REQUIRED FOR LAW ENFORCEMENT TO OBTAIN CELLULAR
LOCATION INFORMATION FROM SERVICE PROVIDERS

As this cellular technology was emerging, police began to request orders for cell phone tracking information, and magistrate judges routinely approved the requests without comment.¹⁵³ In August of 2005, the Eastern District of New York became the first district court to fully examine the issue. In the *Orenstein Opinion*, the government requested real-time cell site information by way of a pen register and a trap and

148. See 18 U.S.C. § 2518 (2006).

149. See *id.* § 2703(d).

150. See *id.* § 3117(a); FED. R. CRIM. P. 41.

151. See 18 U.S.C. § 3122(b)(2).

152. See, e.g., 47 U.S.C. § 1002 (2006); *In re* Application of the U.S. for an Order Directing a Provider of Elec. Comm'n Serv. to Disclose Records to the Gov't, 534 F. Supp. 2d 585, 599 (W.D. Pa. 2008) [hereinafter *Lenihan Order*]; *In re* Application of the U.S. for an Order Authorizing the Use of a Pen Register & a Trap & Trace Device & Authorizing Release of Subscriber Info. &/or Cell Site Info., 384 F. Supp. 2d 562, 563 (E.D.N.Y. 2005) [hereinafter *Orenstein Opinion*].

153. See *Orenstein Opinion*, 384 F. Supp. 2d at 566 (describing how magistrate judges in other jurisdictions are being confronted with the same issue but have not yet achieved consensus on how to resolve it and urging appropriate review of the orders).

trace device.¹⁵⁴ Judge Orenstein admitted that he granted such requests in the past without questioning the legal basis.¹⁵⁵ However, this time he rejected this request and concluded that such orders for real-time cell site information were illegal without a showing of probable cause.¹⁵⁶

Soon after Judge Orenstein's opinion, Judge Smith in the Southern District of Texas issued an opinion that reached the same conclusion based on a different explanation.¹⁵⁷ Judge Smith held that prospective, real-time cell site information fits exclusively into the tracking device category, requiring no less than probable cause.¹⁵⁸ Judge Smith further noted that this technology may raise Fourth Amendment privacy concerns if phones are monitored within an individual's home without her knowledge.¹⁵⁹

Numerous district courts in Maryland, District of Columbia, New York, Indiana, and Wisconsin followed suit, and, over the next three years, eleven opinions were published each holding the government can only obtain prospective, real-time cell site information after receiving a court order based on a showing of probable cause.¹⁶⁰ The most recent

154. *Id.* at 563.

155. *Id.* at 566.

156. *Id.* at 564–65 (holding that the information the government requested would turn the targeted phone into a tracking device, or “an electronic device . . . which permits the tracking of movement of a person or object” (internal quotation marks omitted) (quoting 18 U.S.C. § 3117(b))).

157. *See In re Application for Pen Register & Trap/Trace Device with Cell Site Location Auth.*, 396 F. Supp. 2d 747, 750–57 (S.D. Tex. 2005) [hereinafter *Smith Opinion*].

158. *Smith Opinion*, 396 F. Supp. 2d at 757.

159. *Id.* at 765.

160. *See* McLaughlin, *supra* note 40, at 422–24 & n.11 (summarizing that eleven of the fifteen cell phone location tracking decisions published in the last two years concluded probable cause is required). The eleven decisions are: *In re Application of the U.S. for an Order Authorizing the Release of Prospective Cell Site Info.*, 407 F. Supp. 2d 134 (D.D.C. 2006); *In re Application of the U.S. for an Order Authorizing the Disclosure of Prospective Cell Site Info.*, 412 F. Supp. 2d 947 (E.D. Wis. 2006); *In re Application of the U.S. for an Order Authorizing the Installation & Use of a Pen Register &/or Trap & Trace for Mobile Identification No. (585) 111-1111 & the Disclosure of Subscriber & Activity Info. Under 18 U.S.C. § 2703*, 415 F. Supp. 2d 211 (W.D.N.Y. 2006); *In re Application of the U.S. for an Order Authorizing the Installation & Use of a Pen Register with Caller Identification Device & Cell Site Location Auth. on a Certain Cellular Tel.*, 415 F. Supp. 2d 663 (S.D.W. Va. 2006); *In re Application of the U.S. for Orders Authorizing the Installation & Use of Pen Registers & Caller Identification Devices on Tel. Nos. [Sealed] & [Sealed]*, 416 F. Supp. 2d 390 (D. Md. 2006); *In re Application of the U.S. for an Order: Authorizing the Installation & Use of a Pen Register & Trap & Trace Device; Authorizing the Release of Subscriber and Other Info.; & Authorizing the Disclosure of Location-Based Servs.*, No. 1:06-MC-6, 2006 WL 1876847 (N.D. Ind. Jul. 5, 2006); *In re Application for an Order Authorizing the Installation & Use of a Pen Register & Directing the Disclosure of Telecomms. Records for Cellular Phone Assigned the No. [Sealed]*, 439 F. Supp. 2d 456 (D. Md. 2006); *In re Application of the U.S. for an Order Authorizing Installation & Use of a Pen Register & Trap & Trace Device or Process, Access to Customer Records, & Cell Phone Tracking*, 441 F. Supp. 2d 816 (S.D. Tex. 2006); *In re Application of the U.S. for an Order for Prospective Cell Site Location Info. on a Certain Cellular Tel.*, No. 06 Crim. Misc. 01, 2006 WL 468300 (S.D.N.Y.

published opinion to hold probable cause as the standard for cellular site records came from Judge Lenihan in the Western District of Pennsylvania.¹⁶¹

As courts started to publish opinions in this area, it appeared that a probable cause standard would become the settled consensus. However, courts soon published opinions reaching the opposite conclusion. Now, a majority of courts require probable cause for these orders, but disagreement still exists among the courts.

2. SOME COURTS HAVE HELD THAT A LOWER BURDEN OF SPECIFIC AND ARTICULABLE FACTS IS REQUIRED FOR LAW ENFORCEMENT TO OBTAIN CELLULAR LOCATION INFORMATION FROM SERVICE PROVIDERS

Judge Gorenstein of the Southern District of New York produced the first opinion that reached the conclusion that probable cause was not a required for cell site information.¹⁶² In that case, the government requested real-time information tied to calls from the telephone user, but only sought information from one cell site at a time.¹⁶³ Judge Gorenstein accepted the government's dual-authority argument that such information is available when combining the pen register statute with the Stored Communications Act (SCA), by way of the Communications Assistance for Law Enforcement Act (CALEA).¹⁶⁴ Soon after, the Western District of Louisiana adopted Judge Gorenstein's analysis and allowed the government to receive the same information.¹⁶⁵

Next, the Southern District of West Virginia rejected the dual-authority position, but allowed the government to obtain real-time tracking information based on specific and articulable facts.¹⁶⁶ Most recently,

Feb. 28, 2006); *Orenstein Opinion*, 384 F. Supp. 2d 562; *Smith Opinion*, 396 F. Supp. 2d 747; *In re Application of the U.S. for an Order Authorizing the Installation & Use of a Pen Register & a Caller Identification System on Tel. Nos. [sealed] & [sealed] & the Production of Real Time Cell Site Info.*, 402 F. Supp. 2d 597 (D. Md. 2005).

161. See *In re Application of the U.S. for an Order Directing a Provider of Elec. Commc'n Serv. to Disclose Records to the Gov't*, 534 F. Supp. 2d 585, 616 (W.D. Pa. 2008) (holding that access to records could not be obtained on simple showing of articulable relevance to ongoing investigation and the correct standard is probable cause under Federal Rules of Criminal Procedure 41).

162. See *In re Application of U.S. for an Order for Disclosure of Telecomms. Records & Authorizing the Use of a Pen Register & Trap & Trace*, 405 F. Supp. 2d 435, 450 (S.D.N.Y. 2005) [hereinafter *Gorenstein Opinion*].

163. *Id.* at 437–38.

164. *Id.* at 448–49.

165. See *In re Application of the U.S. for an Order: Authorizing the Installation & Use of a Pen Register & Trap & Trace Device & Authorizing Release of Subscriber Info. &/or Cell Site Info.*, 411 F. Supp. 2d 678, 680 (W.D. La. 2006) (accepting the government's dual-authority position).

166. *In re Application of the U.S. for an Order Authorizing the Installation & Use of a Pen Register with Caller Identification Device & Cell Site Location Auth. on a Certain Cellular Tel.*,

a judge from the Southern District of Texas and a second judge from the Southern District of New York both held that real-time cell site information was obtainable without a showing of probable cause.¹⁶⁷

As courts have furthered arguments for both positions based on a complex statutory backdrop, the current situation remains a live disagreement regarding a significant tool used in police investigations. Further, commentators assert that if the issue is not settled, judges may simply continue to grant these orders without comment.¹⁶⁸ The necessary evidentiary standard must be decided, whether it may be a showing of probable cause, or something less.

V. GPS TRACKING AND CELLULAR PHONE TRACKING IS A SEARCH WITHIN THE MEANING OF THE FOURTH AMENDMENT, REQUIRING POLICE TO OBTAIN A WARRANT BEFORE USE

To determine whether the Fourth Amendment limits police use of GPS and cellular location surveillance methods, we must consider whether the individual being monitored has behaved in a manner that suggests a desire for privacy, and whether the intrusiveness of the technology is significant enough to trigger Fourth Amendment concerns. As discussed below, these questions can be answered in the affirmative based on the existing constitutional framework and the lower and state courts' analysis of the issues.

A. GPS Tracking

Governmental use of GPS devices as a means of obtaining vehicle location information constitutes a search under the Fourth Amendment because the intrusive nature of the technology and the detail of information transmitted invade upon individuals' reasonable expectations of privacy. Therefore, law-enforcement agents should be required to provide a warrant based on probable cause before using this technology.

Again, the basic *Katz* inquiry that the Court will conduct when facing a challenge to a new technology is as follows, "first that a person have an actual (subjective) expectation of privacy, and, second, that the expectation be one that society is prepared to recognize as 'reasonable.'"¹⁶⁹ For constitutional protection to be appropriate, both the subjec-

415 F. Supp. 2d 663, 666 (S.D.W. Va. 2006) (focusing on the fact that the fugitive was using another person's mobile phone and thus was not considered a subscriber under CALEA).

167. See *In re* Application of the U.S. for an Order for Prospective Cell Site Location Info. on a Certain Cellular Tel., 460 F. Supp. 2d 448, 461 (S.D.N.Y. 2006); *In re* Application of the U.S. for an Order: Authorizing the Installation & Use of a Pen Register & Trap & Trace Device, & Authorizing Release of Subscriber & Other Info., 433 F. Supp. 2d 804, 806 (S.D. Tex. 2006).

168. Samuel, *supra* note 48, at 1329–30.

169. *Katz v. United States*, 389 U.S. 347, 361 (1967) (Harlan, J., concurring).

tive and objective prongs must be satisfied. In the context of GPS location tracking, the Supreme Court should find that individuals have met this test.

The first prong of the analysis requires a showing that the individual has behaved in a manner that is consistent with a desire for privacy.¹⁷⁰ This element could be satisfied where law enforcement tracks an individual through an attached GPS device in his or her vehicle. The obvious obstacle to satisfying the first prong, with respect to driving in a vehicle, is that “[a] person traveling in an automobile on public thoroughfares has no reasonable expectation of privacy in his movements from one place to another.”¹⁷¹ It is clear that others are able to view parts of our travels as we pass by on a public street. However, the powerful GPS tracking technology goes well beyond this expected level into an area that most people would consider private. This argument is also strengthened by the fact that the police conduct GPS tracking surveillance for extended periods of time.¹⁷² It is very unlikely that any member of our society believes that merely parking a vehicle on a public street gives law enforcement the right to surreptitiously attach a tracking device without a warrant or consent. Moreover, it is even more improbable that a person would expect to be tracked continuously, twenty-four hours a day, for weeks or months at a time, while a GPS device records all of these travels and thus provides a detailed picture of her private life.¹⁷³ Most drivers would be shocked, if not outraged, to learn that law enforcement has the ability to conduct these activities without any judicial intervention. In GPS tracking cases with this factual scenario, it is likely that a defendant can overcome the subjective-expectation-of-privacy prong of the analysis.

The second prong of the *Katz* inquiry requires a court to determine that a defendant’s expectation of privacy is objectively reasonable, meaning it is one that society is also willing to deem “reasonable.”¹⁷⁴ Additionally, when reviewing this prong, the Supreme Court has considered the level of intrusiveness of the surveillance method, looking specifically to the information that it exposes.¹⁷⁵

When dealing with GPS tracking devices, the objective prong of *Katz* can be satisfied by looking at the intrusive nature of the technology

170. *Id.*

171. *United States v. Knotts*, 460 U.S. 276, 281 (1983).

172. *See State v. Jackson*, 76 P.3d 217, 220–21 (Wash. 2003) (en banc) (describing how the police tracked the defendant’s car for nearly a month after attaching a GPS tracking device).

173. *See id.* at 223 (detailing the powerful capabilities of GPS tracking devices and the privacy concerns arising from police usage).

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

175. *See id.* at 352 (majority opinion); *see also Kyllo v. United States*, 533 U.S. 27, 34 (2001).

and the magnitude of information it reveals. Though GPS devices are known as a type of location tracking device, they are far more advanced than the surveillance methods the Supreme Court has previously addressed. Most notably, this technology is distinguishable from beeper technology, which the Court has characterized as merely sense-augmenting.¹⁷⁶ Beepers require actual and contemporaneous police surveillance, as they function by merely telling how close the police are to the target vehicle based on signal strength.¹⁷⁷ On the contrary, GPS devices do not require police presence in the area; they provide the target's exact coordinates without any additional visual surveillance.¹⁷⁸ Through computer monitoring, police can continuously track the target vehicle for lengthy periods of time as a substitute for visual surveillance.¹⁷⁹ This information is also automatically saved onto the computer database so it is accessible to law enforcement at any time, even months or years later.¹⁸⁰ Moreover, in *Knotts*, the Court specifically addressed the distinction between beeper technology and more intrusive technology. The Court stated that its holding was narrow and should not apply to "dragnet-type" twenty-four-hour surveillance of individuals.¹⁸¹ The characteristics of GPS technology, as a whole, differ from mere sense-augmentation at issue in *Knotts* and place GPS in the category of technology that the Court believed might go beyond the reach of the federal constitution.

For these reasons, GPS surveillance technology better fits into the Court's extrasensory surveillance category, one that requires the procedural safeguard of a warrant prior to police use.¹⁸² In fact, some courts that have dealt with GPS tracking have advocated treating this technology as extrasensory because it operates as a substitute for actual human surveillance.¹⁸³ The extensive level of information collectable through the use of GPS tracking devices without need for visual surveillance, the accuracy of this technology, and the length of uninterrupted surveillance

176. See *Knotts*, 460 U.S. at 282.

177. See *State v. Scott*, No. 02-02-00121-I, 2006 WL 2640221, at *5-6 (N.J. Super. Ct. App. Div. Sept. 15, 2006) (distinguishing beepers from GPS technology).

178. See *Jackson*, 76 P.3d at 223.

179. *Scott*, 2006 WL 2640221, at *6.

180. *Id.*

181. See *Knotts*, 460 U.S. at 284 ("[I]f such dragnet-type law enforcement practices as respondent envisions should eventually occur, there will be time enough then to determine whether different constitutional principles may be applicable.").

182. See *Kyllo v. United States*, 533 U.S. 27, 40 (2001) ("Where . . . the Government uses a device that is not in general public use, to explore details of the home that would previously have been unknowable without physical intrusion, the surveillance is a 'search' and is presumptively unreasonable without a warrant.").

183. See, e.g., *United States v. Berry*, 300 F. Supp. 2d 366, 368 (D. Md. 2004); *Jackson*, 76 P.3d at 223.

substantiates characterizing the technology as extrasensory and providing some constitutional limitation on law-enforcement use.

Furthermore, use of GPS technology is quickly increasing as devices become more affordable and available. Widespread police use of such a powerful technology without judicial supervision could lead to abuse of these devices and trigger the assumption that one's movements are being tracked and recorded at any given moment. This can potentially lead individuals to alter their behavior to accommodate this perception.

The Fourth Amendment protects the features of society that preserve privacy. The original technological inquiry the Court has used since *Katz* informs us that individuals have a reasonable expectation of privacy in the information that police collect through GPS surveillance methods. Thus, law enforcement use of GPS tracking technology is a search, requiring a warrant based on probable cause. With these safeguards in place, judges would ensure that police track a suspect's location only when they possess sufficient justification and only for a period of time appropriate to the purposes of the investigation.

B. *Cellular Phone Tracking*

Like GPS tracking, government acquisition of cellular phone site location information constitutes a search under the Fourth Amendment because it invades upon individuals' reasonable expectations of privacy. Therefore, government agents should be required to provide a warrant based on probable cause before accessing this information.

First, a major privacy concern, which must be addressed, arises because cellular site location information implicates the Fourth Amendment right of privacy in the home. The Supreme Court has clearly recognized the right to privacy in the home as a core Fourth Amendment principle.¹⁸⁴ The Court has also indicated that an objectively reasonable expectation of privacy exists within the home¹⁸⁵ and that collecting data about what takes place inside a home constitutes a search under the Fourth Amendment.¹⁸⁶ This presents a key problem in the context of cell phone location tracking. When law enforcement agents seek cellular location information, they cross the line by learning facts about the interior of the home, which is clearly illegal without a warrant. Because cellular phones travel with the user at all times, they are constantly in

184. *See Kyllo*, 533 U.S. at 31.

185. *See United States v. Karo*, 468 U.S. 705, 714–15 (1984) (“[P]rivate residences are places in which the individual normally expects privacy free of governmental intrusion not authorized by a warrant, and that expectation is plainly one that society is prepared to recognize as justifiable.”).

186. *See id.*

and out of private places, most importantly homes.¹⁸⁷ Cell phone tracking cannot help but implicate the home, as it would be exceedingly difficult to only track a suspect while he was outside the home. Thus, since cell phone tracking will implicate the right of privacy in the home, a warrant should be necessary before engaging in such tracking.

Cellular phone users have a reasonable expectation of privacy in their cellular location information that satisfies the two-prong *Katz* test. First, the subjective portion of the inquiry would almost certainly be met. Many mobile phone users are unaware that law enforcement agents have the ability to track their cellular location information. Further, most cell phone users would surely be astonished, if not angered, to learn that law-enforcement agents can also acquire this information without first obtaining a warrant. A cell phone user understandably views their location information as private and expects it to remain private.¹⁸⁸ As with GPS tracking, cell phone tracking provides an in-depth view into all of a user's private activities and movements, which certainly include a subjective expectation of privacy.

Next, society would determine that a user's expectation of privacy in her cell site location information is objectively reasonable. As discussed, this information reveals details about the inside of the home. The Court has established that society is prepared to recognize expectations of privacy in the home as justifiable.¹⁸⁹ Thus, when the home is implicated, the objective prong of the *Katz* test is satisfied. Moreover, even cellular location information that conveys details about activities outside the home still intrudes upon a user's reasonable expectation of privacy. Though outside of the home, cellular phones follow the user continuously throughout the day, either outside or in private buildings. Law enforcement agents obtain immense detail of the user's daily activities by simply tracking the user's cell location, much of which is sensitive in nature and thought to be private. Similar to GPS tracking, the information obtained from this powerful technology can prove very intrusive when used continuously for long periods of time. Moreover, a majority of the lower courts have taken notice of these important characteristics, holding that a showing of no less than probable cause is the requisite standard for obtaining this cellular location information, with several explicitly finding or strongly implying a reasonable expectation of pri-

187. In fact, many users have cancelled their landline phones and solely use their cellular phones for all communication. Randazzo, *supra* note 30.

188. See *Karo*, 468 U.S. at 735 (Stevens, J., concurring in part and dissenting in part) ("As a general matter, the private citizen is entitled to assume, and in fact does assume, that his possessions are not infected with concealed electronic devices.").

189. See *id.* at 714 (majority opinion).

vacy in this information.¹⁹⁰

Further, when outside the home, cellular phones usually travel in the user's pocket or pocketbook and do not remain in public view. This differentiates the technology and the associated expectation of privacy from beeper cases on public roads.¹⁹¹ The scenario where police obtain cellular location information is more analogous to the situation in *Karo*, where a warrant was required prior to monitoring a beeper that had been "withdrawn from the public view."¹⁹²

Lastly, cellular location information cases cannot be analyzed using the assumption of risk framework from *Smith v. Maryland*, which held that one cannot expect privacy in information voluntarily conveyed to third parties.¹⁹³ To apply *Smith* to cellular tracking, the Court must establish that mobile phone users are aware their location may be tracked and, therefore, assume the risk of continued use. At this time, the Court would not be able to make such a determination. Many users have never considered how their cellular phones work and are unaware that their location can be tracked. Thus, without knowledge of the possible conveyance of information to third-party law-enforcement agents, these cell phone users are not assuming any risk. However, even with future widespread awareness of these capabilities, the information at hand differs greatly from that present in *Smith*. The *Smith* Court focused on the limited nature of the information revealed through use of a pen register, characterizing a pen register as a sense-augmenting device because it discloses solely the number that has been dialed.¹⁹⁴ In contrast, cell phone tracking provides information beyond the numbers dialed, including the contents of the calls; this level of detail crosses the line and falls within the purview of the Fourth Amendment.

Accordingly, since access to cellular phone site location information invades upon individuals' reasonable expectations of privacy and should be deemed a search, government agents must be required to provide a warrant based on probable cause before accessing this information. Judicial authorization would ensure proper, justifiable tracking and protect cell phone users from potential governmental abuse. It is clear that law-enforcement agents can access this cellular location informa-

190. See *supra* notes 153–60 and accompanying text.

191. See *United States v. Knotts*, 460 U.S. 276, 281 (1983) (finding there was no legitimate expectation of privacy while traveling in plain view on public roadways).

192. *Karo*, 468 U.S. at 718.

193. 442 U.S. 735, 744–46 (1979); see also *United States v. Miller*, 425 U.S. 435, 443 (1976).

194. *Smith*, 442 U.S. at 741 (explaining that pen registers did not indicate the actual content of any communication between the caller and recipient, their identities, nor whether the call was even completed).

tion; however, a warrant requirement will ensure they do not circumvent the Fourth Amendment in doing so.

VI. CONCLUSION

Striking the proper balance between individual privacy and the need for protection in the post-9/11 era is a difficult task in a world of ever-increasing technology. The emerging surveillance methods of GPS tracking and cellular phone location tracking provide law-enforcement officers with a variety of ways to complete their objective more efficiently. However, substantial Fourth Amendment concerns are raised by law enforcement's ability to so scrupulously monitor individuals via these technologies without a warrant. Further, because the majority of Americans voluntarily carry cell phones and voluntarily drive cars on a daily basis, these tracking methods are very different from tracking in the past.

Under the traditional *Katz* inquiry, governmental use of both GPS devices and cell phone tracking, as a means of obtaining location information, constitutes a search under the Fourth Amendment. Therefore, law-enforcement agents should be required to provide a warrant based on probable cause before using this technology. The intrusive nature of the technologies and the detail of information transmitted invade upon individuals' reasonable expectations of privacy. Moreover, cell phone tracking implicates the most fundamental Fourth Amendment privacy concern, the right to privacy in the home. Requiring a warrant based on probable cause would save citizens from a world of embarrassment, fear, and privacy invasion.

Due to the severely conflicting views of the lower and state courts, the Supreme Court will likely address these technologies in the near future. Let us hope the Court makes the correct decision, and the police properly use these technologies with the safeguard of a warrant requirement.