Maine Law Review

Volume 64 | Number 1 Article 11

January 2011

The Prolonged Arm of the Law: Fourth Amendment Principles, the Maynard Decision, and the Need for a New Warrant for Electronic Tracking

R. Reeve Wood III
University of Maine School of Law

THE PROLONGED ARM OF THE LAW: FOURTH AMENDMENT PRINCIPLES, THE *MAYNARD* DECISION, AND THE NEED FOR A NEW WARRANT FOR ELECTRONIC TRACKING

Reeve Wood

THE PROLONGED ARM OF THE LAW: FOURTH AMENDMENT PRINCIPLES, THE *MAYNARD* DECISION, AND THE NEED FOR A NEW WARRANT FOR ELECTRONIC TRACKING

Reeve Wood[*]

I. INTRODUCTION

In the fall of 2010, a NPR story recounted how when Yasir Afifi, a California college student of Egyptian extraction, took his car in for an oil change, his mechanic saw a suspicious wire hanging from the bottom of the vehicle.[1] Following the wire, the mechanic located a black object secured to the car with a magnet.[2] When a friend took photographs of the object and posted them on an internet chat site, he was told that the object was a GPS tracking unit.[3] This was confirmed when, several days later, FBI agents and police officers arrived at Afifi's house to reclaim their equipment.[4] To date, Mr. Afifi has not been charged with a crime, but when he filed a FOIA request to uncover information about the FBI's investigation into his activities, the FBI called his counsel and informed them that an investigation was ongoing.[5]

This story, which raises more questions than it answers, illustrates a growing trend in American law enforcement: the deployment of tracking devices capable of recording an individual's travels over long periods of time and relaying location information to officers at the time of their choosing. This kind of device allows for officers to keep tabs on people without having to rely on costly, fallible surveillance performed directly by officers. Instead, tracking devices operate as a sort of "set-it-and-forget-it" surveillance team. The Afifi story would also seem to illustrate another aspect of the growing deployment of tracking devices: the lack of procedural safeguards for those being tracked. In fact, as the issue stands today, in most jurisdictions officers don't even have to talk to a judge, much less get a warrant to install one of these units.[6]

And tracking is not just limited to GPS units placed on cars. Cell phones carry the potential to become tracking devices, snitching from inside the pockets and purses of their owners. Over the last decade, officers have widely requested records of the automatic signals that all cell phones transmit in relaying their

---

* J.D. Candidate, 2012, University of Maine School of Law.

1. Mina Kim, *FBI's GPS Tracking Raises Privacy Concerns*, NAT'L PUB. RADIO (Oct. 27, 2010) http://www.npr.org/templates/story/story.php?storyId=130833487; Kim Zetter, *Caught Spying on Student, FBI Demands GPS Tracker Back*, WIRED (Oct. 7, 2010 10:13 PM), http://www.wired.com/threatlevel/2010/10/fbi-tracking-device.

2. Zetter, *supra* note 1.

3. *Id.*

4. *Id.*

5. Complaint at 2, Afifi v. Holder, No. 11-CV-00460, 2011 WL 726346 (D.D.C. Mar. 2, 2011).

6. *See infra* section IV.B-C.

location information to the service provider. And while they do have to talk to a judge to get this information, in many cases, they don't even have to make a showing of probable cause to obtain an order compelling the release of the data.

While these capabilities aid the ability of police departments and law-enforcement agencies to take on broader investigative burdens, there is something about stories like Mr. Afifi's that unsettles many people. As one circuit court of appeals judge has put it, making the obligatory Orwell reference in the process,

> I don't think that most people in the United States would agree . . . that someone who leaves his car parked in his driveway outside the door of his home invites people to crawl under it and attach a device that will track the vehicle's every movement and transmit that information to total strangers. There is something creepy and un-American about such clandestine and underhanded behavior. To those of us who have lived under a totalitarian regime, there is an eerie feeling of déjà vu . . . . We are taking a giant leap into the unknown, and the consequences for ourselves and our children may be dire and irreversible. Some day, soon, we may wake up and find we're living in Oceania.[7]

Indeed, the ability to easily track the whereabouts of citizens without having to adhere to procedural safeguards of the warrant requirement lends itself to dystopian visions of a state where the government can keep tabs on all its citizens. However, as the findings of the Church Committee on Intelligence Activities demonstrated in 1976, such dark imaginings are not without real grounding in our recent history:

> We have seen segments of our Government, in their attitudes and action, adopt tactics unworthy of a democracy, and occasionally reminiscent of the tactics of totalitarian regimes. We have seen a consistent pattern in which programs initiated with limited goals, such as preventing criminal violence or identifying foreign spies, were expanded to what witnesses characterized as "vacuum cleaners[]," sweeping in information about lawful activities of American citizens.[8]

Despite concerns that tracking technology could open the door to similar government abuses, until recently, courts confronted with tracking technology have largely held that it was excluded from the protections of the Fourth Amendment because tracking individuals in public places did not violate a "reasonable expectation of privacy."[9] However, in August 2010, the Circuit Court of Appeals for the District of Colombia held in *United States. v. Maynard*[10] that the use of a GPS tracking device was a search under the Fourth Amendment.[11] The *Maynard* court provided a rationale for treating prolonged tracking as a search on the grounds that such long-term tracking was able to paint an "intimate picture" of a

---

7. United States v. Pineda-Moreno, 617 F.3d 1120, 1126 (9th Cir. 2010) (Kozinski, J., dissenting).

8. SELECT COMM. TO STUDY GOVERNMENTAL OPERATIONS, 94TH CONG., REP. ON INTELLIGENCE ACTIVITIES AND THE RIGHTS OF AMERICANS § I(A) (1976) [hereinafter Church Committee], *available at* http://www.icdc.com/~paulwolf/cointelpro/churchfinalreportIIa.htm (last visited Apr. 23, 2011).

9. *See* Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan J., concurring) (stating that a government interference is a search where "first, . . . a person ha[s] exhibited an actual (subjective) expectation of privacy and second, . . . the expectation be one that society is prepared to recognize as 'reasonable.'").

10. 615 F.3d. 544 (D.C. Cir. 2010), *cert. granted sub nom.* United States v. Jones, 131 S. Ct. 3064 (June 27, 2011) (No. 10-1259).

11. *Id.* at 555.

person's life, a picture that the individual concerned would not expect others to have sufficient information to piece together.[12] Working as it does within the framework of the established Fourth Amendment jurisprudence, this rationale has been adopted by several federal magistrate judges dealing with the issue of whether the release of cell phone location information constitutes a search and has energized the debate over how courts should deal with electronic tracking. And now, after granting *certiorari*, the Supreme Court will review the D.C. Circuit's decision in *Maynard* (under the case name of *United States. v. Jones*) and pass its ultimate judgment on whether, under this theory, the use of prolonged electronic tracking constitutes a search under the Fourth Amendment.[13]

This article examines the *Maynard* decision as well as the simultaneous emergence of a vocal set of magistrate judges advocating for Fourth Amendment protection for cell phone location information. It argues that, even if the *Maynard* rationale is widely adopted and the use of tracking devices[14] is found to be a search, the Fourth Amendment principles of specificity and limited discretion on the part of government officers mean that the warrant frameworks currently in use will not provide adequate protection from the threat of government officers obtaining information for which they have not demonstrated a need. Finally, it suggests several concepts to be adopted into a new electronic tracking warrant in order to encourage the government to use electronic tracking in a sufficiently focused manner.

Part II provides a brief primer on the origins of the Fourth Amendment and tries to discern basic, overriding principles contained within the amendment, which was largely influenced by a fear of "general warrants" that gave the government broad authority to conduct unspecific searches. Part III tracks the Supreme Court's jurisprudence relating to surveillance technologies. Part IV describes the two most common forms of tracking technology—GPS units and cell phones—and outlines the state of the law around their use, emphasizing the arguments for why their employment should qualify as a search. Finally, Part V examines the types of warrants currently available and proposes a new tracking warrant aimed at minimizing the ability of government officers to capture information that is outside the immediate scope of their investigations.

It should be noted from the outset that this article is specifically concerned with tracking that is "prolonged" in nature. This, of course, invites the dilemma of deciding when tracking becomes "prolonged." Because of the need to provide law enforcement officers with guidance, should such tracking ever be deemed a search under the Fourth Amendment, a bright-line rule will likely be necessary to provide clarity. However, for the purposes of this article, we can proceed with the basic

---

12. *Id.* at 562-64.

13. United States v. Jones, 131 S. Ct. 3064 (June 27, 2011) (No. 10-1259).

14. Fourth Amendment issues are implicated in both the installation and the monitoring of tracking devices. This article will focus strictly on the monitoring or use of these devices as opposed to their physical installation. However, the Supreme Court has ordered the parties in *United States v. Jones* to brief and argue the issue of whether the installation of the tracking device also constitutes a search. *Id.* ("In addition to the question presented by the petition, the parties are directed to brief and argue the following question: 'Whether the government violated respondent's Fourth Amendment rights by installing the GPS tracking device on his vehicle without a valid warrant and without his consent.'").

understanding that "prolonged" tracking is that which continues beyond the duration of a single definable "trip," whether that trip is to the corner store or across the country. With this in mind, we can consider the outer limits of tracking that is not considered "prolonged" to be somewhere around a week. The distinction is important because, as will be discussed below, it is the data produced by prolonged tracking that has the most salient Fourth Amendment implications.

II. THE HISTORICAL BACKGROUND OF THE FOURTH AMENDMENT AND THE FEAR OF GENERAL SEARCHES

The Fourth Amendment of the United States Constitution reads:

> 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.[15]

The Fourth Amendment has been understood to protect the citizen against an unjustified breach of his or her rights of property, autonomy, and privacy by requiring that agents of the government overcome certain procedural hurdles before seizing or searching the citizen or his or her property.[16] Although the current jurisprudential treatment of the amendment is a matter of great debate—one commentator calls it "an embarrassment" and "a mess"[17]—the circumstances that influenced and shaped the amendment are reasonably clear. The particular sort of governmental intrusion that concerned the drafters of the Fourth Amendment was found in the form of "general warrants" and "writs of assistance."[18] The general warrant was a "warrant, general as to the persons to be arrested and the places to be searched and the papers to be seized."[19] As such, a general warrant could not possibly issue on probable cause because it required little or no specificity about who or what was to be arrested or searched.[20] General warrants, however, were limited to "a single specific event that created the cause behind the search."[21] Writs of assistance were a similar device but were subject to even less limitation: a writ of assistance authorized a search anytime during the lifetime of the issuing

---

15. U.S. CONST. amend. IV.

16. *See* CHRISTOPHER SLOBOGIN, PRIVACY AT RISK: THE NEW GOVERNMENT SURVEILLANCE AND THE FOURTH AMENDMENT 23-24 (2007) (describing how the language of the amendment implicates these rights while noting that there is an ongoing scholarly debate over whether the amendment should be read to protect a citizen's privacy). *See also generally* Katz v. United States, 389 U.S. 347 (1967).

17. Akhil Reed Amar, *Fourth Amendment First Principles*, 107 HARV. L. REV. 757, 757, 759 (1994).

18. THOMAS N. MCINNIS, THE EVOLUTION OF THE FOURTH AMENDMENT 15 (2009). *See also* M. Blane Michael, *Reading the Fourth Amendment: Guidance From the Mischief That Gave it Birth*, 85 N.Y.U. L. REV 905, 912 (2010) ("The immediate aim of the Fourth Amendment was to ban general warrants and writs of assistance.").

19. NELSON B. LASSON, THE HISTORY AND DEVELOPMENT OF THE FOURTH AMENDMENT TO THE UNITED STATES CONSTITUTION 43 (De Capo Press 1970) (1937).

20. *Id.*

21. MCINNIS, *supra* note 18, at 43.

sovereign.[22] The practical result of this was that the "discretion delegated to the official was therefore practically absolute and unlimited"; officials could search for contraband whenever and wherever they liked.[23] The extreme power that was granted to the holder of the writ of assistance was hobbled moderately by the fact that the writ did not authorize arrest, and that searches of buildings pursuant to such a writ could only be conducted during the day.[24]

Although the English common law had long been evolving towards a requirement of ex ante review based on probable cause,[25] two English cases from the 1760s solidified the doctrine subsequently enshrined by the Framers in the Fourth Amendment.[26] John Wilkes and John Entick were both newspaper publishers who had produced pamphlets critical of King George III and had been accused of publishing seditious materials.[27] In Wilkes' case, the secretary of state issued a general warrant to search for the "authors, printers, and publishers" of his pamphlet, but did not name Wilkes.[28] Wilkes and forty-nine others were arrested, and his private papers were confiscated.[29] In the case of Entick, a warrant was issued specifying that he be arrested but also ordered that "his papers" be brought before the secretary to be "examined," without specifying which of his papers were to be brought.[30] Predictably, the government officers inspected all of Entick's personal papers and books and confiscated hundreds of pamphlets and charts.[31] Both men sued, and in both cases, the use of the general warrant was found to have been illegal.[32] In upholding a jury's verdict for Entick, Lord Camden of the Court of Common Pleas observed that the law did not allow for a general search as a means of detecting offenders, and that if such a warrant were legal, "the secret cabinets and bureaus of every subject in this kingdom will be thrown open to the search and inspection of a messenger, whenever the secretary of state shall think fit to charge, or even to suspect, a person to be the author, printer, or publisher of a seditious libel."[33] He went on to note that the effect of such a warrant would be to subject a person merely suspected of libel to having "his most valuable secrets . . . taken out of his possession, before the paper for which he is charged is found to be criminal by any competent jurisdiction."[34] "If suspicion at large should be a

---

22. *Id*. at 15-16; LASSON, *supra* note 19, at 53-54.

23. LASSON, *supra* note 19, at 54.

24. *Id.*

25. *Id.* at 35-36 (describing a 17th century treatise in which the English jurist Chief Justice Hale advocated the illegality of general warrants used to search for stolen goods because they did not require that the party asking for the warrant specify the particular place suspected or the probable cause of the suspicion).

26. MCINNIS, *supra* note 18, at 16-17; Eric Schnapper, *Unreasonable Searches and Seizures of Papers*, 71 VA. L. REV. 869, 875-80 (1985).

27. LASSON, *supra* note 19, at 43, 47; Entick v. Carrington, (1765) 95 Eng. Rep. 807 (K.B.) 808; 19 How. St. Tr. 1029, 1031.

28. LASSON, *supra* note 19, at 43.

29. *Id.* at 43-44.

30. *Entick*, 95 Eng. Rep. at 810; 19 How. St. Tr. at 1033-34.

31. *Id.*at 810; 19 How. St. Tr. at 1034-35.

32. Wilkes v. Wood, (1763) 98 Eng. Rep. 489 (K.B.) 499; 19 How. St. Tr. 1153, 1168 (1763); *Entick*, 95 Eng. Rep. at 818; 19 How. St. Tr. at 1074.

33. *Entick*, 19 How. St. Tr. at 1063.

34. *Id.* at 1064.

ground of search . . . whose house would be safe?"[35] These cases were widely publicized and closely followed by both the English public and the inhabitants of the American colonies,[36] and the Supreme Court has recognized *Entick* as having been particularly influential in the formulation of the Fourth Amendment doctrine, stating in 1886 that

> As every American statesmen, during our revolutionary and formative period as a nation, was undoubtedly familiar with this monument of English freedom, and considered it as the true and ultimate expression of constitutional law, it may be confidently asserted that its propositions were in the minds of those who framed the Fourth Amendment to the Constitution, and were considered as sufficiently explanatory of what was meant by unreasonable searches and seizures.[37]

However, the American colonists did not have to look as far as England to find examples of heavy-handed intrusion in the name of law-enforcement. The colonists' interest in the Wilkes and Entick affairs probably reflected the fact that they themselves had been made the subject of such arbitrary intrusion, largely in the form of writs of assistance.[38] In 1761, when customs officers applied to reauthorize their writs following the death of King George II, a group of Boston merchants, represented by James Otis, petitioned the Superior Court against the reauthorization.[39] Arguing against the writs, Otis declared that

> [T]he writ prayed for in this petition, being general, is illegal. It is a power that places the liberty of every man in the hands of every petty officer. I say I admit that special Writs of Assistance, to search special places, may be granted to certain persons on oath; but I deny that the writ now prayed for can be granted . . . .[40]

Otis and the merchants lost, but their arguments "reverberated across America"[41] to the degree that John Adams wrote of Otis's speech that "[t]hen and there the child Independence was born."[42]

These well-worn episodes have been included here because they establish the "point of departure" for Fourth Amendment jurisprudence.[43] They illustrate what

---

35. *Id.* at 1073-74.

36. Schnapper, *supra* note 26, at 912-913; LASSON, *supra* note 19, 45-46; Amar, *supra* note 17, 772 n.54.

37. Boyd v. United States, 116 U.S. 616, 626-27 (1886).

38. For a full account of the use of writs of assistance in the colonies, see LASSON, *supra* note 19, at ch. II, who dedicates a chapter to the topic in his book.

39. LASSON, *supra* note 19, at 57-58; MCINNIS, *supra* note 18, at 18.

40. James Otis, Argument before the Massachusetts Superior Court (Feb. 1761), *available at* http://www.nhinet.org/ccs/docs/writs.htm (last visited Sept. 14, 2011). Part of the text of Otis's actual speech is available, the rest is taken from an account by John Adams, who witnessed it.

41. MCINNIS, *supra* note 18, at 19.

42. William J. Stuntz, *The Substantive Origins of Criminal Procedure*, 105 YALE L.J. 393, 406 n.56 (1995) (citation to footnote only).

43. This view runs counter to a line of scholarship, developed by, among others, Professors Amar and Slobogin, which argues that these historical influences on the Fourth Amendment actually show that the Supreme Court's baseline standard of requiring a warrant and probable cause in order to execute a search or seizure is a misunderstanding of the intent of the Framers, and has resulted in a flaw-ridden Fourth Amendment jurisprudence that, by requiring that such a high burden be met by law enforcement, actually encourages courts to provide exceptions to Fourth Amendment safeguards. *See generally* SLOBOGIN, *supra* note 16; Amar, *supra* note 17.

are arguably a set of normative principles embedded in the Fourth Amendment: in order for the government to interfere with a person's right to be let alone, the government needs to show that it has a strong reason for its interference and that its interference must be directed specifically to deal with this reason. Thus, the government could not search Wilkes's printing presses without there first having been a crime and a certain amount of evidence that Wilkes was involved in that crime. Moreover, even if there was a crime and there was some evidence pointing to Entick's involvement in the crime, the government could not just take all of his papers with an eye toward finding more evidence of his involvement. Rather, the government must be able to specify what evidence it is seeking and narrow its search accordingly. The "security" of the citizenry in their "persons, houses, papers, and effects," is to be maintained by minimizing the amount of discretion that was given to government officials in relation to their investigative and enforcement powers.[44] At bottom, the Fourth Amendment is concerned with government power and its abuse, and a warrant requirement built on specificity and limited discretion is the means by which we have chosen to prevent such abuse.[45]

These principles can be useful when addressing new iterations of the problem of delineating and managing the frontier between the protected privacy of the individual and the need for law enforcement officers to be able to conduct effective investigations. As one Judge has put it, "[t]he Amendment's vivid history can be particularly useful in applying the Amendment to today's challenges and in measuring the consequences of a particular application."[46] In this vein, the Court has not restricted the relevance of these influences to its treatment of the seizure of papers or searches for smuggled goods. As observed below, the ideas embodied in them have been a source of understanding as the Court has dealt with modern iterations of the problem of deciding how a government can go about collecting information about its citizens. However, as its jurisprudence has developed, the potential has emerged for the Court to lose sight of broad Fourth Amendment principles regarding government interference with the "security" of its citizens and focus instead on the vagaries of its own formulations.

III. THE SUPREME COURT AND SURVEILLANCE TECHNOLOGY

This section briefly traces the Supreme Court's jurisprudence relating to surveillance technology. As noted above, the interpretation and application of the Fourth Amendment by the United States Supreme Court has been widely criticized for a perceived incoherence. One of the main difficulties faced by the courts in

---

44. *See* Raymond Shih Ray Ku, *The Founders' Privacy: The Fourth Amendment and the Power of Technological Surveillance*, 86 MINN. L. REV. 1325, 1334 (2002) ("To the extent that the *Wilkes* decision influenced the Founders, it suggests that the Fourth Amendment was adopted as a means of restraining official discretion.").

45. Of course, the wording of the Fourth Amendment does not demand a warrant requirement, but merely requires that searches be reasonable. Professor Amar, among others, argues that we should rid ourselves of the warrant requirement and adopt a more flexible reasonableness standard. *Amar*, *supra* note 17, at 759. *But see* Carol S. Steiker, *Second Thoughts About First Principles*, 107 Harv. L. Rev. 820, 856 (1994) (arguing that the warrant requirement provides a rule-based approach to reasonableness that is necessary in the modern law enforcement context).

46. Michael, *supra* note 18, at 922.

applying the Fourth Amendment has been the development of new technologies that demand an application of the amendment to situations that were unforeseeable by the framers of the Constitution. As the Supreme Court has noted, "The Fourth Amendment is to be construed in the light of what was deemed an unreasonable search and seizure when it was adopted, and in a manner which will conserve public interests as well as the interests and rights of individual citizens."[47] Automobiles, telephones, airplanes, electronic beepers, and thermal imagers have all tested the conception of what it is that the Fourth Amendment protects and what constitutes a search or seizure under the amendment.[48] Evolving social attitudes towards privacy further compound the difficulties associated with technological developments.[49] These factors, combined with the ever-present interest in effective law-enforcement, can make the Fourth Amendment seem like something of a moving target.

Prior to 1967, the Supreme Court had maintained that, in order for surveillance to qualify as a search, and thus engender the protection of the Fourth Amendment, there must be an "actual physical invasion" of a suspect's property.[50] The case that bore the flag for this line of reasoning was *Olmstead v. United States*, in which the Court held that a wiretap of the suspect's phone did not constitute a search under the Fourth Amendment.[51] The Court reasoned that "[t]he language of the amendment cannot be extended and expanded to include telephone wires, reaching to the whole world from the defendant's house or office. The intervening wires are not part of his house or office, any more than are the highways along which they are stretched."[52] In his prescient dissent, Justice Brandeis invoked Chief Justice Marshall's reminder that "it is a *constitution* we are expounding,"[53] and urged that

47. Carroll v. United States, 267 U.S. 132, 149 (1925).

48. *See Carroll*, 267 U.S. at 149 (holding that there was an exception to the warrant requirement in the case of automobiles); Olmstead v. United States, 277 U.S. 455, 465-66 (1928) (holding that a wiretap of a telephone line was not a search regulated by the Fourth Amendment because there was no physical trespass); Katz v. United States, 389 U.S. 347, 353 (1967) (overruling *Olmstead* and finding that a wiretap of a phone booth was a search because the subject of the wiretap had a reasonable expectation to privacy when using a telephone booth); Smith v. Maryland, 442 U.S. 732, 744-45 (1979) (holding that the use of a "pen-register" to record the telephone numbers dialed by a suspect was not a protected search because the suspect had no reasonable belief that those numbers would remain private); Florida v. Riley, 488 U.S. 445, 450-51 (1989) (holding that using a helicopter to fly over a greenhouse in order to look for marijuana was not a search); United States v. Knotts, 460 U.S. 276, 282 (1983) (holding that the use of an electronic beeper to track a car was not a search because the car was exposed to the public on its travels and so there was no reasonable expectation of privacy); United States v. Karo, 468 U.S. 705, 715 (1984) (holding that the use of an electronic beeper to determine if contraband was inside a suspects house was a search under the Fourth Amendment); Kyllo v. United States, 533 U.S. 27, 34-35 (2001) (holding that the use of a thermal imager to scan a suspects house for heat associated with a marijuana growing operation was a search).

49. *See* Susan W. Brenner, *The Fourth Amendment in an Era of Ubiquitous Technology*, 75 MISS. L.J. 1, 40-42 (2005) ("Our interest in, and desire for, privacy increased in the twentieth century, for a variety of reasons. That interest seems to have reached new levels in the early years of the twenty-first century . . . .") (internal citations omitted).

50. *Olmstead*, 277 U.S. at 466.

51. *Id.*

52. *Id.* at 465.

53. *Id.* at 472 (Brandies, J., dissenting) (emphasis in original) (quoting McCulloch v. Maryland, 17 U.S. 316, 407 (1819)).

the constitution be applied in ways that allowed it to bear on developments in surveillance technology.[54] Brandeis also made reference to James Otis and Lord Camden, noting that "writs of assistance and general warrants are but puny instruments of tyranny and oppression when compared with wire-tapping."[55]

In 1967, the Supreme Court turned away from the "physical intrusion" standard. In *Katz v. United States*,[56] a case that involved the wiretapping of a phone booth by law enforcement officers, the Court declared that "the Fourth Amendment protects people, not places," and that "what [a person] . . . seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected."[57] The Court went on to hold that the wiretap was an unreasonable search,[58] and the lasting formulation for determining whether a search has taken place was set forth in Justice Harlan's concurrence. The test, he stated, was twofold: "first, 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.'"[59]

The post-*Katz* Court has examined whether the use of several types of surveillance technology constitutes a search. In *Smith v. Maryland*,[60] the Court held that the use of a "pen-register"—a device that could be installed on the phone company's switching equipment and would record the numbers dialed by a specified telephone[61] -- was not a search.[62] The Court reasoned that, by dialing his phone, the suspect had voluntarily exposed the digits to the switchboard, which was "merely the modern counterpart of the operator who, in an earlier day, personally completed calls for the subscriber."[63] Thus, the suspect could not have harbored an expectation that the numbers he had dialed would remain private.[64]

In *United States v. Knotts*,[65] the case most relevant to the current tracking technologies, the Court held that the use of a "beeper" tracking device was not a search.[66] The government, on suspicion that the defendants were involved in

---

54. *Id.* at 472-74 ("[I]n the application of a constitution, our contemplation cannot be only of what has been but of what may be. The progress of science in furnishing the Government with means of espionage is not likely to stop with wire-tapping.") (internal quotation marks omitted).

55. *Id.* at 476.

56. 389 U.S. 347 (1967).

57. *Id.* at 351. This formulation comes from a concurrence by Justice Harlan. Justice Stewart's opinion for the majority offered a more complex analysis of Fourth Amendment protections, and it is probably owing to this complexity that Harlan's phrasing has been adopted as the meaning of *Katz*. *See* Ricardo J. Bascuas, *Property and Probable Cause: The Fourth Amendment's Principled Protection of Privacy*, 60 RUTGERS L. REV. 575, 583 (2008).

58. *Katz*, 389 U.S. at 359.

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

60. 442 U.S. 735 (1979).

61. *Id.* at 736 n.1.

62. *Id*. at 745-46.

63. *Id.* at 744.

64. *Id.*

65. 460 U.S. 276 (1983).

66. *Id*. at 284-85. The "beeper" in question was a radio transmitter that emitted signals that could be picked up by a receiver held by officers. The purpose of the beeper was to enable the officers to follow the suspects and find them again if they lost visual contact. However, as happened in this case, too great a distance between the transmitter and the receiver would cause the officers to lose the signal. *Id.* at 277-78.

manufacturing drugs, placed the beeper inside a container of chloroform that was then sold to the defendants in Minnesota.[67] Officers followed the defendants from the point of purchase, watched them switch the container into another vehicle, and then followed that vehicle into Wisconsin, where they lost the signal from the transmitter.[68] When a police helicopter equipped with a receiver located the signal again, it was coming from the area around an isolated cabin, which was found to be a drug laboratory.[69] The Court found that the use of the beeper was not a search because the beeper only "augmented" the officers' ability to conduct visual surveillance of the suspects' vehicle, and that because a vehicle "travels public thoroughfares where both its occupants and its contents are in plain view . . . a person traveling in an automobile on public thoroughfares has no reasonable expectation of privacy in his movements from one place to another."[70] Notable, however, was the Court's response to the defendant's argument that unrestricted use of beeper technology would create the possibility of "twenty-four hour surveillance of any citizen of this country . . . without judicial knowledge or supervision."[71] The Court demurred, but it said that "if such dragnet type law enforcement practices . . . should eventually occur, there will be time enough then to determine whether different constitutional principles may be applicable."[72]

In *United States v. Karo*,[73] the Court was again faced with the use of a beeper, but in that case, the law enforcement officers used the beeper signal to show that drug-making chemicals had been taken inside a home in order to obtain a search warrant for the home.[74] In this instance, the Court found that the use of the beeper to signal that an item was inside a home was a search because it conveyed information about the inside of the house that could not have been confirmed visually.[75] Furthermore, "private 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."[76]

Finally, in *Kyllo v. United States*,[77] the Court found that the use of a thermal imaging device to detect heat from the inside of a house was a search under the Fourth Amendment.[78] The Court stated that where the technology is used to "explore details of the home that would previously have been unknowable without

---

67. *Id.* at 278.

68. *Id.*

69. *Id.* at 278-79. The officers used the information gained from following the beeper to obtain a search warrant for the cabin. *Id.* at 279.

70. *Id.* at 281-82. The Court noted that there was no evidence that the beeper had been used to determine the location of the chloroform any more specifically than in the general area of the cabin. *Id.* at 282. However, it implicitly acknowledged that its analysis would have changed had the beeper been used to determine that the container was actually in a private sphere. *Id.* at 281-85.

71. *Id.* at 283.

72. *Id.* at 284.

73. 468 U.S. 705 (1984).

74. *Id.* at 708-10.

75. *Id.* at 715.

76. *Id.* at 714.

77. 533 U.S. 27 (2001).

78. *Id.* at 40.

physical intrusion, the surveillance is a 'search' and is presumptively unreasonable without a warrant."[79] The *Kyllo* court seemed particularly concerned with the fact that the premises at issue was the subject's home, noting that "[a]t the very core of the Fourth Amendment stands the right of a man to retreat into his own home and there be free from unreasonable governmental intrusion,"[80] and that "the Fourth Amendment draws a firm line at the entrance to the house."[81]

Creating a coherent taxonomy of the Court's decisions on surveillance technologies and the Fourth Amendments in order to predict how the Court will rule when faced with a new form of technology is a project that has yielded many different interpretations. In one formulation, the Court's decisions represent a creeping "co-opting" of the *Katz* standard in order to promote a more stringent definition of what qualifies as a constitutionally regulated search than was originally envisioned by the *Katz* court.[82] In this view, the Court's decisions have essentially reverted to a pre-*Katz* definition of a search as relating to an invasion of a "constitutionally protected area" as opposed to the victim's privacy.[83] Thus, in this reading, it is likely that the Court's determination about whether or not the use of a surveillance technology constitutes a search will be premised on the physical area that is being observed.

Another reading of these cases is that they serve to divide technology into two basic categories: that which is "sense augmenting" and that which is "extrasensory."[84] While sense augmenting technology gathers information that "could theoretically be attained through one of the five human senses,"[85] extrasensory technology "reveals information otherwise indiscernible to the unaided human senses."[86] According to this interpretation, the Court generally finds that the use of sense augmenting technologies is less constitutionally objectionable than the use of extrasensory technologies.[87] Importantly, the quantity of evidence obtained by either form of technology will act as a trump card when assessing whether the use of the technology constitutes a search.[88] So under this framework, the determination of whether constitutional protections apply will largely hinge on the invasiveness of a technology as measured in relation to the

---

79. *Id.*

80. *Id.* at 31 (quoting Silverman v. United States, 365 U.S. 505, 511 (1961)).

81. *Id.* at 40 (quoting Payton v. New York, 445 U.S. 573, 590 (1980)).

82. MCINNIS, *supra* note 18, at 241. *See also* SLOBOGIN, *supra* note 16, at 15-16 (describing the tendency of the post-Warren courts to use the *Katz* standard to restrict the regulation of surveillance techniques).

83. MCINNIS, *supra* note 18, at 242 (quoting *Kyllo*, 533 U.S. at 34).

84. Renée McDonald Hutchins, *Tied Up in Knotts? GPS Technology and the Fourth Amendment*, 55 UCLA L. REV. 409, 432-33 (2007). *See also* Ramya Shah, *From Beepers to GPS: Can the Fourth Amendment Keep Up with Electronic Tracking Technology?* 2009 U. ILL. J.L. TECH. & POL'Y 281, 288-89 (2009) (discussing this distinction as applied to GPS tracking in state and lower federal courts).

85. Hutchins, *supra* note 84, at 432-33.

86. *Id.* at 433.

87. *Id*. at 436-37 (discussing *Kyllo* as the primary example of the Court finding that the use of extrasensory technology is a search).

88. *Id.* at 438-42 (noting that the Court has stated hypothetically that the use of sense augmenting technology would constitute a search where it results in an extraordinary quantity of information or unusually detailed information, and that the Court has also found the use of extrasensory technology to be constitutional where the scope of the information it reveals is limited).

normal sensory powers of law enforcement officers, as well as the amount and specificity of the information the technology reveals.[89]

IV. ELECTRONIC TRACKING

While technological development has been a constant throughout the life of the Fourth Amendment, the last quarter of a century has seen a proliferation of devices that, while they enable law enforcement officers to more accurately observe and track suspects, also create opportunities for "[s]ubtler and more far-reaching means for invading privacy."[90] Such devices include powerful cameras equipped with biometric face-recognition software, the thermal imagers mentioned above, and detection devices that enable law enforcement officers to essentially see through clothing in order to find secreted contraband or weapons. The focus of this article will be on recently-developed electronic systems that enable law enforcement officers to track the location of a civilian over an indefinite length of time.

A. The Technology

1. GPS Tracking Units

One of the most effective and cost-efficient technologies being adapted for law enforcement purposes is global positioning system technology ("GPS"). Originally developed by the Defense Department for military uses, GPS systems allow a receiver on earth to communicate with multiple satellites orbiting the earth on specified pathways.[91] By triangulating its location in reference to the satellites, the receiver is able to plot its position on the earth's surface to within two meters.[92] A GPS receiver can also record latitude, longitude and altitude, as well as direction and speed of movement.[93] A transmitter in the receiver can then relay the information contained therein to a monitoring party. This can be done either by real-time monitoring of the receiver or through periodic wireless uploads of information stored in the receiver's memory.[94] The receiver's memory can also be recovered when the receiver is physically retrieved. Notably, there is no limit to the number of GPS receivers that can be in communication with GPS satellites at any one time.[95]

The most common use of a GPS receiver by law enforcement personnel—at least as evidenced by the number of court cases in which the technology is an issue—is to track the vehicle of a person or persons of interest.[96] A GPS receiver

89. Hutchins does note that the area being observed can also be a factor in determining whether a search has occurred, primarily when that area is a home. *Id.* at 442-43.

90. Olmstead v. United States, 277 U.S. 438, 473 (1928) (Brandeis, J., dissenting).

91. Hutchins, *supra* note 84, at 414-18.

92. *Id.*

93. *Id.* at 418.

94. Shah, *supra* note 84, at 284-85 (internal citations omitted).

95. Hutchins, *supra* note 84, at 418.

96. *See, e.g.*, United States v. Maynard, 615 F.3d 544 (D.C. Cir. 2010), *cert. granted sub nom.* United States v. Jones, 131 S. Ct. 3064 (June 27, 2011) (No. 10-1259); United States v. Marquez, 605 F.3d 604 (8th Cir. 2010); United States v. Pineda-Moreno, 591 F.3d 1212 (9th Cir. 2010); United States v. Garcia, 474 F.3d 994 (7th Cir. 2007); United States v. McIver, 186 F.3d 1119 (9th Cir. 1999); United

can easily be affixed to a suspect's vehicle, and the vast majority of courts have held that the actual application of the device to the vehicle does not constitute a search or seizure, so long as it occurred on the street or in the suspect's driveway.[97]

While efforts to obtain data on the frequency of the use of GPS tracking by law enforcement have largely been frustrated, there are indications that it is becoming widespread practice.[98] The Department of Justice has encouraged police departments to invest in GPS tracking devices by helping to foot the bill for the units.[99] Such a proliferation is to be expected because the devices are cheap, available, efficient, and largely infallible.[100] In the surveillance context, GPS devices do not require sleep, meals, refueling, or bathroom breaks, and a suspect is less likely to notice that she is being monitored when the observer is a miniscule device attached to the underside of her car than when it is a bleary-eyed detective or surveillance team tailing her throughout her daily travels.[101]

Of course, the qualities that make a GPS receiver so attractive as a tool for law enforcement also make the technology an item of particular constitutional concern. It is subject to none of the practical limitations that serve to discourage employing physical surveillance by officers without a very strong reason for believing that the suspect has engaged in criminal behavior and that the surveillance will reveal evidence of that behavior.[102] It can be deployed for as long as desired with a

---

States v. Jesus-Nunez, No. 1:10-CR-00017-01, 2010 WL 2991229 (M.D. Pa. July 27, 2010); United States v. Burton, 698 F. Supp. 2d 1303 (N.D. Fla. 2010); United States v. Moran, 349 F. Supp. 2d 425 (N.D.N.Y. 2005); Commonwealth v. Connolly, 913 N.E.2d 356 (Mass. 2009); People v. Weaver, 909 N.E.2d 1195 (N.Y. 2009); People v. Gant, No. 05-0196, 2005 N.Y. Misc. LEXIS 1604 (N.Y. Co. Ct. 2005); People v. Lacey, No. 2463N/02, 2004 WL 1040676 (N.Y. Co. Ct. 2004); Foltz v. Commonwealth, 698 S.E.2d 281 (Va. App. 2010); State v. Jackson, 76 P.3d 217 (Wash. 2003).

97. *See, e.g.*, *Pineda-Moreno*, 591 F.3d at 1215 (holding that, where the tracking device was installed while the suspect's car was in his driveway, there was no reasonable expectation of privacy because the suspect had not made any showing that his driveway was in any way protected from the public view or access); *Garcia*, 474 F.3d at 996 (holding that "the defendant's contention that by attaching the memory tracking device the police searched his car is untenable."); *McIver*, 186 F.3d at 1126-27 (holding that the installation of a tracking device on a suspect's car was not a search because the officers did not enter the curtilage of the suspect's home, and because the suspect had no reasonable expectation of privacy regarding the underside of his vehicle because the underside still constituted part of the car's exterior). *But see* Commonwealth v. Connolly, 913 N.E.2d. 356, 369-70) (Mass. 2009) (holding on state law grounds that installation of a GPS unit on the defendant's car was a seizure of the car).

98. Ben Hubbard, *Police Turn to Secret Weapon: GPS Device*, WASH. POST, Aug. 13, 2008, at A1.

99. Press Release, U.S. Dep't of Justice, Justice Department Awards More than $570,000 to Area Law Enforcement Agencies to Combat Gangs (Apr. 14, 2008), *available at* www.justice.gov/usao/iln/pr/chicago/2008/pr0414_01.pdf.

100. A brief search of the Internet located commercially available GPS tracking units intended for covert use for as low as $199. *GPS Tracking Devices*, BRICKHOUSE SECURITY, http://www.brickhousesecurity.com/gps-car-tracking-vehicle-logging.html (last visited Oct. 10, 2011).

101. *See* State v. Jackson, 76 P.3d 217, 223 (Wash. 2003) (noting that it is unlikely that officers could have "maintained uninterrupted 24-hour surveillance" of a suspect who was tracked by a GPS device).

102. *See* Bennett L. Gershman, *Privacy Revisited: GPS Tracking as Search and Seizure*, 30 PACE L. REV. 927, 951 (2010) (noting that it would be "inconceivable . . . . given budgetary constraints on police work, finite time pressures for different and competing investigations, and limited police personnel," that officers using physical surveillance techniques would have been able to gather the same quality and quantity of evidence used against a suspect as was gathered by a GPS device).

minimal investment of time or money: the initial cost of the unit, a change of batteries when required, and the effort to upload the information from the receiver and review it.[103] The use of a GPS tracking unit does not, theoretically, even require that anyone really ever monitor it until they think that they have a reason for doing so. The unit will passively and comprehensively record the data it is designed to collect, whether or not that information has any real law-enforcement purpose. The effect of these characteristics is that vast amounts of information about a subject can be gathered in a relatively easy and wholly undiscerning manner, and, as will be discussed later, such aggregations of information make it possible for law enforcement to learn much more about a person than just their physical location.[104] Furthermore, these characteristics make it easy for people who are uncomfortable with the idea of such profound governmental access to information about where its citizens are and what they are doing to envision a scenario in which, if left unchecked, all citizens are monitored by the state to ensure that they are not engaging in activities that the state does not approve of: the dystopian vision of Orwell or Huxley.

2. Cell Phones as Tracking Devices

A second form of tracking device is carried in the purses and pockets of the vast majority of Americans.[105] The standard cellular phone operates by constantly "registering" with the nearest cellular tower or "base station" so that incoming and outgoing calls can be accurately directed to and from the phone unit through the tower from which the phone receives the strongest signal.[106] As the phone unit moves and the strength of the signal with one tower declines, the signal is switched to a closer tower.[107] The record of a phone's registration with nearby towers is called the "cell site" data or the "cell site location information" (CSLI).[108] The general location of a phone can be determined by locating the tower providing the signal to the phone (more specifically, which "sector" or "face" of the tower the phone is communicating with) and by measuring the strength of the signal.[109]

Thus, like bread crumbs along a path, as a person moves through his day, his phone is communicating with cell towers, creating a potential record of his movements.[110] The precision of this method of tracking the location of a phone

---

103. *See* William R. Wright, *Vehicle Tracking Surveillance; Is it Legal?*, 26 MATRIMONIAL STRATEGIST 1 (2008) (noting that trackers are available that run either on disposable batteries or rechargeable batteries).

104. *See infra* note 159 and accompanying text.

105. "As of December 2009, more than 90 percent of the overall population of the United States subscribed to cell phone service—an estimated 285.6 million people." Catharine Crump & Christopher Calabrese, *Location Tracking: Muddled and Uncertain Standards Harm Americans' Privacy*, 88 CRIM. L. REP. 19 (2010).

106. Kevin McLaughlin, *The Fourth Amendment and Cell Phone Location Tracking: Where Are We?*, 29 HASTINGS COMM. & ENT. L.J. 421, 426 (2007).

107. *Id.*

108. Crump & Calabrese, *supra* note 105.

109. McLaughlin, *supra* note 106, at 426-27; Crump & Calabrese, *supra* note 105.

110. Recent Developments, *Who Knows Where You've Been? Privacy Concerns Regarding the Use of Cellular Phones as Personal Locators*, 18 HARV. J.L. & TECH. 307, 309 (2004).

unit is variable depending on how many towers service a given location.[111] Where, as in urban environments, there are more towers, each tower services a smaller area and thus a phone's location can be more accurately plotted.[112] Inversely, where there are fewer towers, each tower covers a larger area and the range in which a specific phone could be located based on its communications with the tower is broader.[113] There has been a steady trend towards the placement of more towers or base stations in densely populated environments in order to provide service for increasing numbers of cell phone users.[114] As the number of base stations in an area increases, the smaller each "sector" becomes, and the more precise the location of a cell phone will be in relation to the sectors it is communicating with.[115]

The use of data from several towers, through a process of "triangulation," can produce even more accurate information about the location of a cell phone.[116] By measuring the time it takes a phone's signal to reach multiple towers or the angle at which the signal reaches the towers, it is possible to plot the location of the phone to within 50 meters.[117] In addition to triangulation, extremely accurate tracking of cell phone location is being facilitated by the proliferation of GPS receivers installed in phones. In response to the Wireless Communications and Public Safety Act of 1999, the FCC promulgated regulations requiring that, by 2005, wireless carriers had to be able to provide emergency services with the accurate location of any cell phone user who called 911.[118] This can be accomplished either through the use of triangulation or by the inclusion of a GPS chip inside a cell phone.[119]

One important difference between tracking performed through the use of a GPS receiver that is installed by law enforcement officers on a suspect's vehicle, for example, and tracking using a suspect's cellular phone is that in the latter case the authorities do not have direct access to the data—they must instead deal with an intermediary, the service provider, to obtain the information. Authorities may request either "historical" data, which is used to locate a person's past locations, or "prospective" data, which allows real-time tracking of a suspect.[120] As will be discussed below, government requests for location data are subject to an uncertain statutory framework. However, it is clear that there is not currently a uniform

---

111. Crump & Calabrese, *supra* note 105.

112. *Id.*

113. *Id*.

114. *In re* United States for Historical Cell Site Data (*Smith II*), 747 F. Supp. 2d 827, 832 (S.D. Tex. 2010). Because the case names in the government's requests for orders to disclose CSLI information are somewhat unwieldy, they have been replaced here with the name of the issuing (or denying) judge and a roman numeral indicating the specific order's place in the chronology of orders by the same judge that are referenced in this paper.

115. *Id.*

116. *In re* Application of U.S. for an Order for Prospective Cell Site Location Information on a Certain Cellular Telephone (*Kaplan I*), 460 F.Supp.2d 448, 451 (S.D.N.Y. 2006).

117. *Id.*; Crump & Calabrese, *supra* note 105.

118. *9-1-1 Service*, FEDERAL COMMUNICATIONS COMMISSION, http://transition.fcc.gov/pshs/services/911-services (last visited October 10, 2011); James X. Dempsey, *Digital Search & Seizure: Updating Privacy Protections to Keep Pace with Technology*, 865 PLI/PAT 505, 531 (2006).

119. Darren Handler, Note, *An Island of Chaos Surrounded By a Sea of Confusion: The E911 Wireless Device Location Initiative*, 10 VA. J.L. & TECH. 1, ¶¶ 17-18 (2005).

120. Crump & Calabrese, *supra* note 105.

requirement that a warrant based on probable cause must issue in order to obtain cell phone tracking information.[121]

Another distinction between the two technologies is that, while a person who has had a GPS tracker surreptitiously attached to their vehicle has not intended to broadcast their patterns of travel, a person who makes a call using a cellular phone does so with (perhaps a vague) notion that the phone is sending and receiving signals in such a way that would probably require a cellular network, in some manner, to know its general location. Whether or not this distinction is significant for Fourth Amendment analysis will also be discussed below.

The constitutional concerns surrounding the use of cell phones as tracking devices are perhaps even greater than those relating to the use of a GPS unit attached to a vehicle. First, by virtue of possessing a cell phone, nearly every American adult can now be tracked by the government.[122] Furthermore, not only can the government gain access to a citizen's real-time movements from the point at which it becomes interested in tracking the person, but it can also obtain data by which it can account for the movements of a person in the past.[123] This, combined with increased cell-tower density and the fact that improvements in GPS technology allow ever increasing tracking accuracy, means that cell phones have become a means by which law enforcement could access a nearly unlimited agglomeration of the type of data that concerned the *Maynard* court.[124]

B. The Treatment of GPS Tracking in the Circuit Courts of Appeal

As noted above, the circuit courts and state supreme courts are currently split on whether or not the use of GPS tracking devices by law enforcement officers constitutes a search. With relative economy of space in mind, this survey will only examine decisions by circuit courts of appeal as these cases are representative of the broader arguments made at all levels.

The circuit courts have been presented with both the question of whether the attachment of the GPS unit is a search as well as whether its use to record information is a search, but only the decisions examining use, i.e. monitoring, will be dealt with here. The courts have dealt with these questions in varying detail but have found in three cases that use of the devices was not a search under the Fourth Amendment.[125] Only in *Maynard* did a circuit court find that the use of a GPS tracking unit was a search.[126]

---

121. *See In re* Application of the U.S. for an Order (1) Authorizing the Use of a Pen Register & a Trap & Trace Device (*Orenstein I*), 384 F. Supp. 2d 562, 566 (E.D.N.Y. 2005) (describing how the presiding federal magistrate judge had previously authorized court orders for cell site information without questioning the constitutionality of the release of such information without a warrant based on probable cause).

122. Crump & Calabrese, *supra* note 105.

123. *Id.*

124. *See infra* note 159 and accompanying text.

125. *See generally* United States v. Marquez, 605 F.3d 604 (8th Cir. 2010); United States v. Pineda-Moreno, 591 F.3d 1212 (9th Cir. 2010); United States. v. Garcia, 474 F.3d 994 (7th Cir. 2007).

126. United States v. Maynard, 615 F.3d 544 (D.C. Cir. 2010), *cert. granted sub nom.* United States v. Jones, 131 S. Ct. 3064 (June 27, 2011) (No. 10-1259).

1. GPS tracking is Not a Search

In the cases where circuit courts found that the use of a GPS tracker was not a search, their decisions were generally premised on an extension of the Supreme Court's holding in *Knotts*.[127] In extending *Knotts*, the courts made little or no distinction between the beeper device at issue in that case and a GPS unit. Nor did these courts distinguish between the relatively short period of tracking in that case and the weeks or months of tracking at issue in the cases before them.

In *United States v. Marquez*, the Eighth Circuit considered the use of a GPS device, albeit in a rather roundabout way.[128] In that case, Drug Enforcement Agency (DEA) agents attached a GPS tracker to a vehicle that they suspected was involved in drug trafficking.[129] The defendant was arrested after the investigators used the device to track the use of the truck in a drug conspiracy in which he was involved.[130] When the defendant tried to challenge the legality of the use of the device without a warrant, the court found that he did not have standing to challenge its use.[131] However, the court, citing *Knotts*, stated that even if the defendant had standing, the use of the GPS device would not have been a search because "[a] person traveling via automobile on public streets has no reasonable expectation of privacy in his movements from one locale to another."[132] Significantly, the court made no attempt to distinguish the GPS device at issue in the case from the beeper unit used in *Knotts*.

In *U.S. v. Pineda-Moreno*, the Ninth Circuit also failed to make a meaningful inquiry into the differences between the older beeper units and units utilizing GPS.[133] In that case, DEA agents observed the defendant purchasing large quantities of fertilizer "of a type frequently used to grow marijuana."[134] After identifying the defendant, learning where he lived, and obtaining more evidence indicating that he was involved in growing marijuana, agents attached a GPS

---

127. See *supra* Part III.

128. 605 F.3d 604.

129. *Id.* at 607.

130. *Id.* The court does not state precisely how long the subjects in this case were tracked, however the court does relay that the batteries on the GPS unit were replaced seven times, and that the agents first placed the device on the vehicle in May 2007, and the subjects were arrested in October 2007. *Id.*

131. *Id.* at 609. The court found that the defendant lacked standing because he did not own the vehicle and was only "an occasional passenger therein." *Id.*

132. *Id.* (internal citations omitted). Interestingly, the court did require that officers have reasonable suspicion prior to installing the device, although there does not appear to have been any requirement of an *ex ante* showing before the installation. *Id.* at 610. Although the court cites to *Garcia* for this proposition, Judge Posner's opinion in that case appears to only note that the district court judge overseeing the initial motion to suppress in *Garcia* found that reasonable suspicion was a sufficient quantum of proof on which to predicate the installation of a tracking device. United States v. Garcia, 474 F.3d 994, 996 (7th Cir. 2007). The district court judge, in one of her orders on the defendant's motion to suppress, states that she adopted the reasonable suspicion requirement on the recommendation of the magistrate judge. United States v. Garcia, No. 05-CR-0155-C-01, 2006 WL 1601716, at *1 (W.D. Wis. May 31, 2006). The district court judge suggested that the court would require an *ex ante* showing in the future. *Id.* This rather *ad hoc* process of establishing a standard illuminates the need for judicial clarity when addressing the question of just what oversight should be applied to electronic tracking.

133. 591 F.3d 1212 (9th Cir. 2010).

134. *Id.* at 1213.

device to his vehicle.[135] Using multiple tracking units, the agents monitored the defendant's travels over the course of four months and finally arrested him after a tracking device showed that he was leaving a suspected marijuana "grow-site."[136] After arresting the defendant, agents found a considerable amount of marijuana at his home.[137] The defendant argued that the agents' monitoring of the device had been a search because *Kyllo* had "heavily modified" the analysis used by *Knotts*, and under *Kyllo*, the GPS unit would qualify as an extrasensory technology.[138] The court disabused the defendant of this notion, holding that *Kyllo* did not apply because the GPS units at issue were not extrasensory technology[139] but were, in fact, sense-augmenting technology because they only allowed the agents to obtain the same information that they would have gained by physically following the defendant.[140] The court went on to hold that, because this sense-augmenting technology was not deployed against a "constitutionally protected area," its use could not be a search.[141]

Finally, in *United States v. Garcia*, the case that contains the most considered defense of the use of GPS tracking without a warrant, the Seventh Circuit recognized that the beeper used in *Knotts* was a "less sophisticated device" than a GPS unit and that GPS tracking holds the potential for "wholesale surveillance."[142] However, in a somewhat cavalier opinion authored by Judge Posner, the court decided that it need not address "[w]hether and what kind of restrictions should, in the name of the Constitution, be placed on such surveillance when used in routine criminal enforcement," because the officers involved in the case had "abundant grounds for suspecting the defendant" prior to subjecting him to GPS tracking.[143] The defendant in the case had come under the police's suspicion after several informants had told police officers that he was intent on manufacturing methamphetamine, and he was observed purchasing ingredients for the drug.[144] Officers installed a GPS unit on the defendant's car, and, as a result of tracking the

---

135. *Id.* The court's opinion only calls the devices that the agents used in this case "tracking devices." However, the court discusses how the devices retained a record of the defendant's travels, which the agents could access either when they retrieved the units or remotely. *Id.* at 1213, 1216. This indicates that the units used by the agents were GPS units as opposed to beeper units.

136. *Id.* at 1213-14.

137. *Id.* at 1214.

138. *Id.* at 1216.

139. The court here used the term "sense enhancing" as opposed to "extrasensory," but the meaning is the same in relation to technology that is "sense augmenting." *See supra* Part III.

140. *Pineda-Moreno*, 591 F.3d at 1216. The court viewed the information obtained through the use of the tracking devices in its narrowest sense, stating that, "[t]he only information the agents obtained from the tracking devices was a log of the locations where Pineda-Moreno's car traveled . . . ." *Id.* As will be described below, this narrow view is at odds with the position taken by some courts, which is that the information made available through electronic tracking depicts a much broader range of behavior than just the physical locations that a person visited. Especially in cases like this, where the tracking is conducted over a span of multiple months, those doing the tracking can divine a person's habits, religious and political preferences, medical issues and much more.

141. *Id.*

142. 474 F.3d 994, 997-98 (7th Cir. 2007).

143. *Id.* at 998.

144. *Id.* at 995.

defendant's travels, were able to discover his methamphetamine lab.[145] Judge Posner found that the use of the GPS to track the defendant was merely a technological improvement on physical surveillance performed by officers and that "the [fourth] amendment cannot sensibly be read to mean that police shall be no more efficient in the twenty-first century than they were in the eighteenth."[146]

2. GPS Tracking is a Search

At the time of writing, there has only been one case in which a circuit court, utilizing a theory that had been developed in several state court opinions,[147] has found that the use of a GPS tracking unit for a prolonged period of time is a search. Because the reasoning used in this decision informs the central thesis of this paper, and because it provides an ample discussion of most of the arguments for finding that such use of GPS is a search, the court's analysis will be examined in more detail than the decisions discussed above.

In 2010, the D.C. Circuit, in *United States v. Maynard*, found that *Knotts* did not apply where law enforcement officers used GPS tracking to monitor the movements of a suspect over the course of a month, and that the use of the device for a prolonged period of time constituted a search under the Fourth Amendment.[148]

---

145. *Id.* Judge Posner's opinion does not say how long the defendant was tracked using GPS.

146. *Id.* at 998. By way of illustration, Judge Posner states that similar updates to manned surveillance include the use of cameras mounted on lamp posts and satellite imaging "as in Google Earth." *Id.* at 997. Judge Posner's use of these technologies as examples would seem to provide a false mark for measuring whether GPS tracking represents an increase in invasiveness over current technologies that do not require a warrant. Firstly, while real-time satellite-image tracking of a suspect would raise all the same constitutional concerns as GPS tracking and more, to this Author's knowledge, Google Earth does not provide live satellite pictures that would enable tracking. A search of case law and other sources turns up no indication that Google Earth or any other live satellite imaging technology has been applied by domestic law enforcement agencies to follow a suspect in real-time. Secondly, while cameras mounted on stationary lamp-posts may implicate constitutional concerns, their use arguably does not carry the same potential for invasiveness that is the worrying feature of GPS tracking.

147. These cases include Commonwealth v. Connolly, 913 N.E.2d 356 (Mass. 2009), People v. Weaver, 909 N.E.2d 1195 (N.Y. 2009), and State v. Jackson, 76 P.3d 217 (Wash. 2003), all of which are referred to in *Maynard*. In *Jackson*, the Washington Supreme Court found that a GPS device attached to the car of a suspected murderer did not merely augment officers' senses, but instead recorded the suspect's position regardless of "whether an officer could in fact have maintained visual contact over the tracking period." 76 P.3d at 223. The court was also concerned by the potential for GPS tracking to reveal "a great deal about an individual's life," including their "preferences, alignments, associations, personal ails and foibles." *Id.* Likewise, in *Weaver*, the New York Court of Appeals voiced its concern about the "[c]onstant, relentless tracking" that GPS makes possible. 909 N.E.2d at 1199. The court found that GPS represents even more than an "enhancement" of the officers' senses, "it facilitates a new technological perception of the world in which the situation of any object may be followed and exhaustively recorded over, in most cases, a practically unlimited period." *Id.* In both *Jackson* and *Weaver*, the courts found that their respective state constitutions required that authorities obtain a warrant before using GPS tracking. *Jackson*, 76 P.3d at 224; *Weaver*, 909 N.E.2d at 1203. In *Connolly*, the Massachusetts Supreme Judicial Court—applying a less-restrictive definition of seizure than have federal courts—found that the placement of a GPS tracker on a vehicle was a seizure under the Massachusetts constitution because, "by using the GPS device on the vehicle to track its movements the police asserted control over it, converting the minivan to their own use notwithstanding the defendant's continued possession." 913 N.E.2d at 370.

148. 615 F.3d 544, 555-56, 563 (D.C. Cir. 2010), *cert. granted sub nom.* U.S. v. Jones, 131 S. Ct. 3064 (June 27, 2011) (No. 10-1259).

In that case, a combined FBI-DC Metropolitan Police Department task force investigating the owner and manager of a nightclub for suspected drug trafficking used a GPS unit to track the whereabouts of the nightclub owner's vehicle around the clock for four continuous weeks.[149] The pattern of the defendant's travels became one of the central pillars of the government's case against him.[150] When the defendant appealed his conviction based on the use of this evidence, the government argued that, under *Knotts*, the GPS device was not a search because the defendant had no reasonable expectation of privacy during his trips on public roadways.[151] Unlike the other circuit courts that have evaluated GPS tracking in light of the Fourth Amendment, the D.C. Circuit found that the difference in technology between the *Knotts* beeper and a GPS unit—particularly the capability of a GPS unit to enable officers to monitor a suspect's movements for prolonged periods of time—was fundamental enough that the Fourth Amendment analysis that applied to the one could not be readily transferred to the other.[152] The *Maynard* court specifically focused on the *Knotts* court's caveat that should "twenty-four hour surveillance of any citizen of this country . . . be possible without judicial knowledge or supervision," then "different constitutional principles may be applicable."[153] Accepting this invitation, the *Maynard* court took a fresh look at the *Katz* test as it applied to prolonged GPS tracking.

The court in *Maynard* began by defining the "information" that the defendant claimed was private.[154] Whereas in *Knotts* the information at issue was the defendant's movement between two locations, in *Maynard* the information that the defendant argued was private was the record of his total travels over the course of the twenty-eight days he was monitored.[155] The court then examined whether or not the defendant had exposed this information to the public, either actually or constructively, on the theory that, if he had done so, he could not have had a reasonable expectation to privacy, per the *Katz* standard.[156] The court found that the defendant had not actually exposed the totality of his movements over the course of the month because such exposure, in Fourth Amendment terms, only occurs where a person reasonably expects that others will observe it, and in this case, the defendant could not reasonably expect that any individual citizen would

149. *Id.* at 549, 555.

150. *Id.* at 562 n.*.

151. *Id.* at 556.

152. *Id.* at 556-58.

153. *Id.* at 556 (citing United States v. Knotts, 460 U.S. 276, 283-84 (1982)). The *Knotts* Court also referred to this twenty-four hour surveillance as "dragnet type law enforcement practices." *Knotts*, 460 U.S. at 283. The *Maynard* court explicitly notes that this language from the *Knotts* Court is in response to an argument from the defendant in that case that the beeper would enable round the clock tracking of individual citizens. *Maynard*, 615 F.3d at 556-57, n.*. This is important, because other courts seem to have read the *Knotts* Court's use of the phrase "dragnet type law enforcement practices" to refer to a program of mass surveillance. *See* United States v. Walker, 771 F. Supp. 2d 803, 811 (W.D. Mich. 2011) (applying the *Knotts* "dragnet" language to "shotgun tactics" where officers attach devices to multiple vehicles and wait to see "which device leads to evidence of a potential criminal violation.").

154. 615 F.3d at 558.

155. *Id.*

156. *Id.*

observe all of his travels over the course of a month.[157]

Significantly, the court also stated that precedent appeared to foreclose any argument that, by exposing each of his individual trips, the defendant had constructively exposed the whole pattern of his travels during the time he was tracked.[158] The basis of this finding was that the whole pattern of travel reveals more information than would any one of its constituent parts.[159] As the court stated, this kind of long-term, unblinking surveillance

> reveals types of information . . . such as what a person does repeatedly, what he does not do, and what he does ensemble. These types of information can each reveal more about a person than does any individual trip viewed in isolation. Repeated visits to a church, a gym, a bar, or a bookie tell a story not told by any single visit, as does one's not visiting any of these places over the course of a month. The sequence of a person's movements can reveal still more; a single trip to a gynecologist's office tells little about a woman, but that trip followed a few weeks later by a visit to a baby supply store tells a different story. A person who knows all of another's travels can deduce whether he is a weekly church goer, a heavy drinker, a regular at the gym, an unfaithful husband, an outpatient receiving medical treatment, an associate of particular individuals or political groups—and not just one such fact about a person, but all such facts.[160]

Having determined that the defendant did not expose the entire pattern of his travels to the public, the court then turned to whether or not his expectation of privacy in his travels over the course of the four weeks he was monitored was, in fact, reasonable.[161] In what is probably the most vulnerable part of its opinion, the court concluded that the fact that several states had passed laws creating civil or criminal sanctions for private use of GPS tracking units and requiring warrants for

---

157. *Id.* at 558-60. The court recognized implicitly that the first prong of the *Katz* test, the question of whether the subject has manifested an expectation of privacy, has less bearing in cases of prolonged surveillance. As Professor Hutchins puts it, while a defendant trying to suppress evidence obtained through a very brief, *Knotts*-style period of tracking would be expected to offer "some evidence of surreptitious behavior, . . . as the period of targeted surveillance becomes more protracted (as is possible with GPS-enabled tracking), a countervailing reality must be acknowledged--that citizens of this country largely expect the freedom to move about in relative anonymity without the government keeping an individualized, turn-by-turn itinerary of our comings and goings."
Hutchins, *supra* note 84, at 455.

158. *Maynard*, 615 F.3d. at 560-63. It should be noted that the government did not make a "constructive exposure" argument, so this section of the court's analysis is essentially dicta.

159. *Id.* at 561-62. Dicta or not, this "aggregation theory" of the use of surveillance technology is notable for directly and clearly addressing what commentators see as one of the principal threats of prolonged tracking. *See* April A. Otterberg, Note, *GPS Tracking Technology: The Case for Revisiting* Knotts *and Shifting the Supreme Court's Theory of the Public Space Under the Fourth Amendment*, 46 B.C. L. REV. 661, 696-97 (2005) ("Even though one may expect fleeting glances in public, and police should not have to avert their eyes from what they can see in public, one does not thereby expect the kind of targeted aggregation of data a GPS device collects on one's movements, particularly a kind of surveillance the individual neither can detect nor prevent."); Hutchins, *supra* note 84, at 458 (observing that GPS tracking enables law enforcement to compile a record, not only of comings and goings, but also of "friends, associates, preferences, and desires.").

160. *Maynard*, 615 F.3d at 562.

161. *Id.* at 563.

government use of such devices,[162] as well as the fact that several state courts have found that GPS tracking by law enforcement requires a warrant,[163] was "indicative that prolonged GPS monitoring defeats an expectation of privacy that our society recognizes as reasonable."[164]

Next, the court addressed the distinction between prolonged surveillance using GPS, and physical surveillance conducted by law enforcement officers. The government argued that the rationale employed in finding the use of GPS units to be a search would have the effect of making officers' visual surveillance of public acts also qualify as a search.[165] The court reaffirmed that its holding was grounded in the fact that the reasonable expectation at issue was not whether someone would observe a single trip from one place to another, but whether someone would observe all of the defendant's trips for a month, and that this did not implicate brief instances of visual surveillance.[166] The court also indicated that it need not address instances of prolonged visual surveillance that might have mirrored the facts in the case at hand, if for no other reason than that the government had made no showing that such surveillance was ever used, and that the potential for such surveillance was severely constricted by the enormous amount of resources it would demand and the inherent difficulty in conducting successful long-term surveillance.[167]

Finally, and most importantly, the court distinguished between GPS surveillance and visual surveillance on the grounds that the Supreme Court's treatment of surveillance technologies had determined that "when it comes to the Fourth Amendment, means do matter."[168] For instance, where an undercover officer wore a wire and recorded a suspect, there was no search, but where the same information was obtained through a wiretap, the Court found that there had been a search.[169] "Quite simply, in the former case one's reasonable expectation of control over one's personal information would not be defeated; in the latter it would be."[170]

Based on its findings that the defendant had possessed a reasonable expectation of privacy in the totality of his movements over the course of four weeks and that he had not exposed this larger pattern of movement to the public, the Circuit Court of Appeals for the District of Columbia found that law

---

162. *Id.* at 564 (citing UTAH CODE ANN. §§ 77-23a-4, 77-23a-7, 77-23a-15.5 (LexisNexis 2010); MINN. STAT. §§ 626A.37, 626A.35 (2010); FLA. STAT. §§ 934.06, 934.42 (2010); S.C. CODE ANN. § 17-30-140 (2010); OKLA. STAT. tit. 13, §§ 176.6, 177.6 (2010); HAW. REV. STAT. §§ 803-42, 803-44.7 (2010); 18 PA. CONS. STAT. § 5761 (2010)).

163. *Id.* (citing State v. Jackson, 76 P.3d 217, 223-24 (Wash. 2003); People v. Weaver, 909 N.E.2d 1195, 1203 (N.Y. 2009); Commonwealth v. Connolly, 913 N.E.2d 356, 369-70 (Mass. 2009)).

164. *Id.* The court, however, did acknowledge that these indicators are "not conclusive evidence of nationwide societal understandings." *Id*. (internal quotation marks omitted).

165. *Id.* at 565.

166. *Id.*

167. *Id.* The court noted that a Special Agent involved in the investigation of the defendant had said during the trial: "Physical surveillance is actually hard, you know. There's always chances of getting spotted, you know, the same vehicle always around, so we decided to use GPS technology." *Id.* at 565 n.* (citations omitted).

168. *Id.* at 566.

169. *Id.* (citing Lopez v. United States, 373 U.S. 427, 429 (1963); Katz v. United States, 389 U.S. 347, 353 (1967)).

170. *Id.*

enforcement officers had conducted a warrantless search of the defendant when they tracked him using GPS technology and, because the defendant had been convicted based on evidence obtained through that search, overturned his conviction.[171]

There is little indication that the "aggregation theory" announced by the D.C. Circuit in *Maynard* will be adopted widely in regard to GPS tracking units or that the decision will even stand.[172] Only guidance from the Supreme Court or Congress will go any length in settling the matter. However, the decision in *Maynard* is an important one. It is an attempt, within the current framework of Fourth Amendment jurisprudence, to give voice to a widely held belief that, at least in normative terms, the Constitution was designed to keep the government from monitoring its citizens to the degree that it would be able to learn their secrets without showing good reason for needing to do so. The line over which the Government was not to step was much clearer when people's secrets were kept locked away in desk drawers, and the practical demands of physical, man-to-man surveillance meant that the government was more likely to be judicious in monitoring its citizens' activities. Tracking technology has changed this dynamic, and the *Maynard* decision presents a method of framing the threat posed by GPS tracking in a way that brings that threat under the powers of the Fourth Amendment. The *Maynard* rationale has also proved to be helpful to courts dealing with another form of electronic tracking, one that poses arguably more threat to the privacy of citizens and also is regulated by a more complex legal framework: cell phone tracking.

C. Cell Phones as Tracking Devices: Statutory Framework and Divided Treatment in the District Courts

Courts' treatment of the use of cell-phones as tracking devices, both for prospective and historical location data, differs fundamentally from their treatment of GPS tracking units because of the existence of a hodgepodge of relevant federal statutes governing telecommunications as well as the requirements of the Federal Rules of Criminal Procedure. The fact that cell phones are so widely owned and do not have to be installed onto the property of the suspect makes them appealing as tracking devices, but the trade-off for law-enforcement officers is that the information they are trying to obtain[173] is in the possession of a third party, the cellular service provider, and a court-order is necessary under the relevant statutes in order to compel the service provider to give out this information. It is the request for such a court order, usually from a federal magistrate judge, that provides the forum for the judiciary's determination of what restrictions, either statutory or stemming from the Fourth Amendment, apply to cell phone location data. The quantum of proof required for the government to acquire this data is far

171. *Id.* at 568.

172. The Justice Department's original petition for certiorari for *Maynard* was denied. Maynard v. United States, 131 S. Ct. 671 (2010) (mem.). However, on June 25, 2011, the Supreme Court granted *certiorari* in the case of *United States v. Jones*, the case of the specific defendant whose tracking was at issue in *Manyard*. United States v. Jones, 131 S. Ct. 3064 (June 27, 2011) (No. 10-1259).

173. *See* discussion in *supra* Part IV.A.2.

from a settled question. As one federal magistrate judge who is prominently involved in this issue has said, "[e]ach year . . . busy magistrate judges issue hundreds of ex parte cell phone tracking orders, with literally no appellate guidance concerning the proper threshold showing for their issuance--probable cause versus something less."[174]

The following sections will discuss the statutory framework applicable to government use of cell-phone location data, specifically CSLI. It will then discuss the differing ways in which the courts have interpreted this framework when confronting requests for both prospective and historical data, and will note a growing trend in recent years towards requiring a showing of probable cause in order for law enforcement officers to compel release of cell phone location information.

1. The Statutory Framework

The main body of law that bears on the use of cell phones as tracking devices is the Electronic Communications Privacy Act of 1986 (ECPA).[175] The three components of ECPA are Title I: The Amended Wiretap Act,[176] Title II: The Stored Communications Act,[177] and Title III: The Pen/Trap Statute.[178] These statutes set forth a system whereby the standard of proof necessary for the government to obtain information rises, roughly, in correspondence to the private nature of the information sought and the invasiveness of the means of obtaining it.

The Pen/Trap Statute demands the lowest standard of proof on the part of the government. Under the statute, if the government makes a showing that the "information likely to be obtained . . . is *relevant to an ongoing criminal investigation*," then the court is required to issue an order allowing the government to install a pen-register or trap-and-trace device.[179] These devices are used to identify the source-device of communications coming to a suspect's phone or computer or the intended recipient-device of communications sent by the suspect, but are not meant to capture the actual content of the communications.[180]

The Communications Assistance for Law Enforcement Act (CALEA)[181] affects the implementation of the Pen/Trap Statute, requiring that "information acquired solely pursuant to the authority for pen registers and trap and trace devices . . . shall not include any information that may disclose the physical location of the subscriber (except to the extent that the location may be determined from the telephone number)."[182] This statute explicitly shuts off the possibility that law enforcement will be able to obtain CSLI through a pen/trap order.

---

174. Stephen Wm. Smith, *Kudzu in the Courthouse: Judgments Made in the Shade*, 3 FED. CTS. L. REV. 177, 212 (2009).

175. Pub. L. No. 99-508, 100 Stat. 1848 (1986) (codified throughout title 18 U.S.C.).

176. 18 U.S.C.A. §§ 2510-2522 (West 2011).

177. *Id.* §§ 2701-12.

178. *Id.* §§ 3121-27.

179. *Id.* § 3123(a)(1) (emphasis added).

180. *Id.* § 3127(3)-(4).

181. 47 U.S.C.A. §§ 1001-10 (West 2011).

182. *Id.* § 1002(2)(B).

Under the Stored Communications Act (SCA), records related to electronic communication

> may be issued by any court that is a court of competent jurisdiction and shall issue only if the governmental entity offers *specific and articulable facts* showing that there are reasonable grounds to believe that the contents of a wire or electronic communication, or the records or other information sought, are relevant and material to an ongoing criminal investigation.[183]

Importantly, the definition of "electronic communication" specifically excludes "any communication from a tracking device."[184]

Finally, the Amended Wiretap Act requires that, in order to intercept the contents of any electronic communications, the government must make a showing necessary to meet the "super warrant" requirements outlined in 18 U.S.C. § 2518, including a "particular description of the type of communications sought to be intercepted."[185] A court order for a wiretap can only issue upon a finding by the judge that, among other factors, there is probable cause to believe both that a suspect "has committed, or is about to commit a particular offense" and that communications related to that offense will be intercepted.[186] The extra requirement that gives this procedure its nickname is that the government must show that "normal investigative procedures have been tried and have failed or reasonably appear to be unlikely to succeed if tried or to be too dangerous."[187] Because the Amended Wiretap Statute governs the interception of "content," it is not at issue when considering orders for CSLI, although some groups have argued that it should be.[188]

In addition to the statutory requirements of the ECPA, Federal Rule of Criminal Procedure 41 states that "a magistrate judge with authority in the district has authority to issue a warrant to install within the district a tracking device,"[189] and that "[a]fter receiving an affidavit or other information, a magistrate judge . . . must issue the warrant if there is probable cause to . . . install and use a tracking device."[190] Thus, although the discussion above demonstrates that there is no current statutory requirement that a warrant be issued in order to use a tracking device, pursuant to this rule, any federal court order for the use of a tracking device requires a showing of probable cause.

It is within the framework provided by these statutes and rules that government officers and judges, without the benefit of any real appellate oversight, have tried to

---

183. 18 U.S.C.A. § 2703(d) (emphasis added) (incorporating the definition of "electronic communication" found at 18 U.S.C.A. § 2510(12)).

184. *Id.* § 2510(12)(c). 18 U.S.C.A. § 3117(b) defines a tracking device as "an electronic or mechanical device which permits the tracking of the movement of a person or object."

185. 18 U.S.C.A. § 2518(1)(b)(iii).

186. *Id.* § 2518(3)(a)-(b).

187. *Id.* § 2518(3)(c); *In re* Application of the U.S. for an Order (1) Authorizing the Use of a Pen Register & a Trap & Trace Device (*Orenstein II*), 396 F. Supp. 2d 294, 305 (E.D.N.Y. 2005) (describing the difference in requirements between an ordinary Rule 41 warrant and a "super warrant").

188. *See* Brief for The Electronic Frontier Foundation as Amicus Curiae Opposing the Government, at section III.B, *Orenstein I*, 384 F. Supp. 2d 562 (E.D.N.Y. 2005) (arguing that cell phone tracking implicates the same privacy concerns that led to the creation of the wiretap act).

189. FED. R. CRIM. P. 41(b)(4).

190. FED. R. CRIM. P. 41(d)(1).

determine what level of proof is necessary in order to secure an order compelling the release of cell phone location data. The following sections will outline the approaches to this issue taken by federal magistrate judges, and will note the emergence of a vocal group of magistrate judges who require a showing of probable cause in order to issue an order to release CSLI.

2. Prospective Location Information

The issue of how to deal with government requests for prospective CSLI—that is, court orders for service providers to turn over data on communication between a suspect's handset and cell towers that would occur in the future—appears to have largely emerged in 2005, apparently due to the efforts of several federal magistrate judges.[191] Government requests for prospective CSLI data are based on one of two grounds: 1) pursuant to the SCA alone, arguing that the CLSI constituted records of electronic communications under the SCA, and could be released by the provider pursuant to an order obtained on the basis of a "specific and articulable facts" standard,[192] and 2) pursuant to a combination of the Pen/Trap Statute and the SCA, which would also apparently provide the authority for the government to obtain prospective CSLI with a "specific and articulable facts" showing (this is known as the "hybrid theory").[193]

Confronted with these arguments, magistrate judges have examined each

---

191. There do not appear to be any published opinions on the issue prior to 2005. This probably owes to the fact that opinions on the matter were sealed or otherwise unreported, and the indication is that, prior to 2005, government requests for CSLI were routinely granted. Recognizing this, Federal Magistrate Judges James Orenstein of the Eastern District of New York and Stephen WM. Smith of the Southern District of Texas both went to the apparent extra effort of making their opinions on the orders public and instigating a transparent judicial debate on the issue. *See Orenstein I*, 384 F. Supp. 2d 562, 566 (E.D.N.Y. 2005) (noting that the magistrate judge had found no federal case law on point, although he did acknowledge having previously "granted applications for similar relief, as recently as April 1, 2005, without questioning the legal basis for doing so or suggesting that there might be none"); *In re* Application for Pen Register and Trap/Trace Device with Cell Site Location Authority (*Smith I*), 396 F.Supp.2d 747, 748-49, 749 n.1 (S.D. Tex. 2005) (stating that the case under consideration appeared to be a matter of first impression in that circuit, that the only reported decision on the issue was *Orenstein I*, and that because of the importance of the issue, and despite sealing the underlying order, he would not seal his opinion on the case).

192. *Orenstein I*, 384 F. Supp. 2d at 563. Judge Orenstein mistakenly stated that the government was attempting to classify CSLI as "*contents* of . . . electronic communication" under § 2703(a) of the SCA. *Id.* (emphasis added). He acknowledged this mistake in his reconsideration of the request, which contains a more detailed account of his rejection of the request for an order for CSLI, noting that CSLI would be a record of electronic communication, as opposed to the contents of that communication. *Orenstein II*, 396 F. Supp. 2d at 302 n.4. *See also Smith I*, 396 F. Supp. 2d at 749.

193. *Orenstein II*, 396 F. Supp. 2d at 315 (the government did not use the hybrid theory in their initial application for an order, but argued that it applied when Judge Orenstein granted a reconsideration of his original order); *Smith I*, 396 F. Supp. 2d at 761; In re Application of U.S. for an Order Authorizing Installation and Use of a Pen Register and a Caller Identification System on Telephone Numbers [sealed] (*Bredar I*), 402 F. Supp. 2d 597, 600 (D. Md. 2005). The basis of the hybrid theory is CALEA's amendment of the Pen/Trap Statute so that location information cannot be given out by a provider based "solely" on a pen/trap authorization. 47 U.S.C. § 1002(2)(B). The government relies on the word "solely" to imply that, under CALEA, the combination of the Pen/Trap Statute and the SCA provide sufficient authority to obtain prospective cell site data. For a clear and detailed explanation of the hybrid theory, see *Smith I*, 396 F. Supp. 2d at 761.

relevant statute to determine which, if any, could support an order for issuing CSLI. They have concluded that the Pen/Trap statute, as amended by CALEA, was unable to do so based on the express language stating that information obtained "solely" pursuant to a pen/trap authorization could not contain location data.[194] The SCA would seem to provide the best fit for authorizing CSLI, but the Judges have found that it was not up to the task on two grounds: 1) because it contains an exclusion relating to records of electronic communications from tracking devices, CSLI could not be obtained under the SCA because the release of that data would arguably turn the phone into a tracking device,[195] and 2) because the SCA deals with "records" of electronic communications, it can only authorize the release of information relating to communications that have already happened.[196]

Finally, most magistrate judges who have published opinions on the matter seem to have dismissed the hybrid theory[197]—in which the combination of the SCA and the Pen/Trap statute would allow the SCA to lend the Pen/Trap Statute the added authority that the "solely" language of CALEA seems to demand, while the Pen/Trap Statute would provide the SCA with the prospective focus that it clearly lacks—as being somewhat too fanciful. Magistrate Judge Smith, in a rationale that has been widely adopted, points specifically to the facts that none of the statutes reference each other[198] and that the various statutes were enacted over the course of 15 years and in an order that defies the apparent logic of the hybrid theory.[199]

Based on this evaluation of the statutory framework, most magistrate judges who have published opinions have found that the standard of proof required to obtain an order authorizing the release of prospective CSLI is probable cause as demanded by Federal Rule of Criminal Procedure 41.[200] However, several magistrate judges have, in published opinions, accepted the hybrid theory and have

---

194. *Orenstein I*, 384 F. Supp. 2d at 565; *Smith I*, 396 F. Supp. 2d. at 757-58; *Bredar I*, 402 F. Supp. 2d at 603.

195. *Orenstein I*, 384 F. Supp. 2d at 563-64; *Smith I*, 396 F. Supp. 2d. at 759.

196. *Smith I*, 396 F. Supp. 2d at 760-61.

197. Patrick T. Chamberlain, Note, *Court Ordered Disclosure of Historical Cell Site Location Information: The Argument for a Probable Cause Standard*, 66 WASH. & LEE L. REV. 1745, 1768-69 (2009) ("Generally, the government has had very little success in compelling the disclosure of real-time CSLI by way of its hybrid theory argument."). *But see* Christopher Soghoian, *8 Million Reasons for Real Surveillance Oversight*, SLIGHT PARANOIA (Dec. 1, 2009), http://paranoia.dubfire.net/2009/12/8-million-reasons-for-real-surveillance.html (stating that location information can often be gained through a hybrid order, and referring to a presentation given by a telecom industry lawyer who stated that each major wireless service provider receives over 100 requests a week for location information).

198. *Smith I*, 396 F. Supp. 2d at 764 ("Surely if these various statutory provisions were intended to give birth to a new breed of electronic surveillance, one would expect Congress to have openly acknowledged paternity somewhere along the way.").

199. *Id.* at 765. Smith notes that, while the "solely" language in CALEA is supposed to be the proverbial key to the lock of the hybrid theory, CALEA went into effect in 1998. *Id.* It wasn't until a 2001 Patriot Act amendment to the Pen/Trap Statute, making it apply to "electronic communications," that the CALEA language could have any effect on CSLI.

200. Adam Koppel, Note, *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, 1082 (2010) (noting that "a majority of courts require probable cause for these orders" but also noting a continued disagreement among the districts). *See also* Chamberlain, *supra* note 197 at 1748 n.19 (noting that, as of April 2009, of the 28 reported decisions on prospective CSLI, 20 had found that probable cause was required to obtain a court order releasing the information).

issued orders for the release of prospective CSLI on the basis of a showing of "specific and articulable facts."[201] Notably, however, these courts have also emphasized that their decisions were also based on the fact that in their cases the government was seeking, or their orders allowed, a less invasive level of CSLI. For instance, the decisions involved only the data relating to the duration of phone calls, and then only information relating the cell tower actually directing the call to the phone, as opposed to the three points necessary for triangulation.[202] These courts argue that the limited level of CLSI released to the government means that there is no "tracking" precise enough to create a Fourth Amendment issue where the release of CLSI has been authorized with a sub-probable-cause showing.[203] Furthermore, these courts argue that CLSI that is related to a cell phone as it is being used to make or receive calls does not convert that cell phone into a "tracking device" as contemplated by the Supreme Court.[204] Instead of a device being installed by the government, here "the individual has chosen to carry a device and to permit transmission of its information to a third party, the carrier."[205] Thus, the most appropriate analogy would be to the pen register at issue in *Smith v. Maryland*, where the Supreme Court found that a suspect had no expectation to privacy in the phone numbers he dialed because he knowingly exposed them to a third party.[206] Although the reasoning of the courts demanding a probable cause standard for the release of prospective CSLI largely avoids this question, it takes up a more prominent role in the debate over the standard of proof necessary to obtain a release of historical CSLI.

3. Historical Location Information

The terms of the debate over whether probable cause is required for an order to release historical CSLI (records of cell site registrations occurring prior to the

---

201. *In re* Application of U.S. for an Order for Disclosure of Telecommunications Records and Authorizing the Use of a Pen Register and Trap and Trace (*Gorenstein I*), 405 F. Supp. 2d 435, 438-49 (S.D.N.Y. 2005); In re Application of the United States for an Order (*Hornsby I*), 411 F. Supp. 2d 678, 679-81 (W.D. La. 2006).

202. *Gorenstein I*, 405 F. Supp. 2d at 437-38; *Hornsby I*, 411 F. Supp. 2d at 680 ("The Government's application in this case seeks only the same information (by type and degree) allowed by Magistrate Judge Gorenstein.").

203. *Gorenstein I*, 405 F. Supp. 2d at 449 ("[T]he data being sought by the Government in this District is not what *amicus* believes it to be. The information does not provide a "virtual map" of the user's location. The information does not pinpoint a user's location within a building. Instead, it only identifies a nearby cell tower and, for some carriers, a 120-degree face of that tower. These towers can be up to 10 or more miles apart in rural areas and may be up to a half-mile or more apart even in urban areas. Moreover, the data is provided only in the event the user happens to make or receive a telephone call. Thus, *amicus'*s reference to tracking devices and the cases considering this technology is not on point.").

204. *Id.* To make this case, Judge Gorenstein relies on a reading of *Karo* in which it was the installation of the beeper, as opposed to its monitoring, that was at issue. *Id.* at 449.

205. *Id.*; *see also Hornsby I*, 411 F. Supp. 2d at 681 ("A cell phone is not a tracking device as that term is commonly understood. Tracking devices are devices that are "installed" at the request of the Government. Cell phones are not "installed." They are carried (usually in a person's pocket or purse) and used voluntarily. Any cell phone user who has ever had a call dropped due to a lack of service knows that their cell phone communicates with the nearest tower.").

206. 442 U.S. 735, 744 (1978).

application for a court order) are largely the same as those referred to above.[207] However, as Magistrate Judge James Orenstein has noted, when dealing with historical records, the SCA more readily applies due to its retrospective orientation.[208] Because of this, according to Magistrate Judge Stephen Wm. Smith, "most courts to date have granted government access to such information under the SCA ."[209] However, the statutory issue is not necessarily conclusive, and the courts that have required probable cause for the release of historical CSLI have largely done so on the grounds that to release such information implicates the Fourth Amendment. As one magistrate judge puts the argument, release of historical CSLI based on a less demanding standard would

> violate Americans' reasonable expectation of privacy in any cell-phone-derived information/records as to their physical movements/locations by authorizing *ex parte* disclosure of that information with no judicial review of the probable cause. It appears to this Court, from its review of current Fourth Amendment case law and Constitutional principles, that this information is entitled to the judicial-review protections afforded by a probable cause warrant and historically applied to movement/location information derived from a tracking device.[210]

This view has been supported by the one circuit court that has reviewed a request for an order to release historical CSLI, which stated that, unlike the suspect in *Smith v. Maryland*, cell phone users are not generally aware that the company stores information about their location even when their phone is not in use, and so "[a] cell phone customer has not 'voluntarily' shared his location information with a cellular provider in any meaningful way."[211]

For the courts which, like the Third Circuit, distinguish CSLI from the pen register at issue in *Smith*, the D.C. Circuit's decision in *Maynard* has provided further justification for questioning the constitutionality of historical CLSI obtained

---

207. For a comprehensive explanation of the rationales on both sides of the CSLI discussion as it stood through 2008, see Chamberlain, *supra* note 197, at 1775-88.

208. *In re* Application of U.S. for an Order Authorizing Release of Historical Cell-Site Information (*Orenstein III*), 736 F. Supp. 2d 578, 580 (E.D.N.Y. 2010) ("I have previously concluded—and continue to believe—that as a statutory matter the SCA permits a court to issue the order the government now seeks without a showing of probable cause.").

209. *Smith II*, 747 F. Supp. 2d at 830 (referencing several recent cases from other federal district courts.).

210. In re U.S.for an Order Directing a Provider of Electronic Communication Service to Disclose Records to the Government (*Lenihan I*), 534 F. Supp. 2d 585, 610-11 (W.D. Pa. 2008) *rev'd*, 620 F.3d 304 (3rd Cir. 2010).

211. *In re* U.S. for an Order Directing a Provider of Electronic Communication Service to Disclose Records to the Government (*Sloviter I*), 620 F.3d 304, 317-18 (3rd Cir. 2010). Interestingly, the Third Circuit overturned the magistrate judge's decision in *Lenihan I* requiring a showing of probable cause, determining instead that the text of § 2703(d) required a showing of articulable facts at a minimum, and gave judges the discretion to require a showing necessary for a warrant. *Id.* at 319. The court clearly implied that one of the considerations in determining whether a warrant was required would be the Constitutional consequences of the government's request. *Id.* at 317-19. *See also Smith I*, 396 F. Supp. 2d at 756-57 (referring to the Sixth Circuit's decision in *United States v. Forrest*, 355 F.3d. 942, 951-52 (6th Cir. 2004) by saying "the Sixth Circuit was persuaded that *Smith* did not extend to cell site data" because "cell site data is not 'voluntarily conveyed' by the user to the phone company . . . it is transmitted automatically during the registration process, entirely independent of the user's input, control, or knowledge.").

without a showing of probable cause. Magistrate Judges Orenstein and Smith have both issued opinions stating that the theory undergirding *Maynard*[212]—what Orenstein calls the "intimate portrait theory"—is relevant and instructive in regard to historical CSLI, and its application compels a finding that government acquisition of historical CSLI can constitute a search under the Fourth Amendment.[213] In reaching this conclusion, Magistrate Judge Orenstein found no distinction based on the real-time nature of the tracking at issue in *Maynard* and the retrospective nature of the CSLI being contemplated in the case before him.[214] The "intimate picture" painted by prolonged surveillance "is no less intimate simply because it has already been painted."[215] Furthermore, he found that there was no distinction between the invasion of privacy caused by GPS and that caused by CSLI.[216] Nor did he find that the subject of tracking had a more reasonable expectation of privacy in his vehicle than he did relating to his cell phone.[217]

The law on what standard of proof is required for the government to obtain cell phone location data is still a murky pool. A majority view that probable-cause is required in the case of prospective CSLI may have coalesced, but it is by no means unanimous. Things are even less clear when it comes to historical CSLI. While it is likely that the majority of magistrate judges will still grant orders for the release of historical CSLI based on a showing of articulable facts, there is a growing clamor being raised by the same magistrate judges who chose to broadcast their reasons for requiring probable-cause in order for the government to obtain prospective CSLI. The probable-cause position also seems to have been energized by the *Maynard* decision and the Third Circuit's decision in *Sloviter I*. One thing, however, is for sure: for at least six years, magistrate judges and district courts, joined in 2010 by a circuit court, have been appealing to Congress to bring clarity to these questions.[218] Without a definitive solution, it seems likely that many magistrate judges will continue to grant orders for CSLI based on a showing of articulable facts without issuing opinions and that prosecutors will venue-shop to

---

212. *See* discussion of *Maynard supra* Part IV.B.2.

213. *See Orenstein III*, 736 F. Supp. 2d at 582, 596; *Smith II*, 747 F. Supp. 2d at 838.

214. *Orenstein III*, 736 F. Supp. 2d at 585 ("The fact that the government seeks information that has already been created says nothing about whether its creator has a reasonable expectation of privacy in that information.").

215. *Id.*

216. *Id.* at 589-91. The government's premise on this count was that CSLI could not locate a subject as accurately as GPS, and that, in this case the only data requested was that generated while the phone was making or receiving calls, and so its use did not rise to the level of a search. *Id.* at 589-90. Magistrate Judge Orenstein noted the increasing accuracy of CSLI, and found no distinction between the limitations of CSLI data obtained only during calls, and the GPS tracking in *Maynard*, which only tracked the vehicle itself and did not account for the suspect when he was on foot. *Id.* at 590-91.

217. *Id.* at 592-594. The government argued that a telephone user has less of a reasonable expectation of privacy regarding their telephone's location than a driver does their vehicle's location because a cell phone user "should know" that when they place a call the service provider is informed of the cell tower being used. *Id.* at 592. Magistrate Judge Orenstein acknowledged the most cell phone users are aware of the possibility that their phones can divulge their location to the service provider, but stated that the increase in location-based services in phones has corresponded with an expectation among consumers that this tracking technology could be controlled or turned off, and that the dissemination of location data was subject to their approval. *Id.* at 593.

218. *See* Chamberlain, *supra* note 197, at 1788-89 (describing the need for a legislative solution).

the extent possible until they find the magistrate judge who will get them the information they want with the minimal showing necessary. One commentator has proposed a simple statutory fix, whereby Congress pass a single statute to the effect of:

> (a) A court shall not grant a Government application to compel disclosure of cell site location information, whether real-time or historical, and shall not otherwise order disclosure of such information, except upon a showing of probable cause as authorized by Rule 41 of the Federal Rules of Criminal Procedure.
> (b) This law shall serve as the sole authority upon which a court may order disclosure of real-time and/or historical cell site location information.[219]

Such a legislative solution would certainly go a long way in improving the protection of individuals' privacy interests, but, as discussed below, it might still fall short of the principles embodied in the Fourth Amendment.

V. THE NEED FOR A SPECIAL TRACKING WARRANT

So where do we stand now? In most jurisdictions, government officers do not need a warrant to install and monitor a GPS device on a suspect's vehicle, tracking that individual wherever they drive for as long as the officers like. There are concerns, however, that the prolonged tracking of individuals using this kind of technology represents an invasion of a sphere in which the tracked individual has a reasonable expectation of privacy that society is prepared to recognize—the totality of their movements over an extended period of time—and now the *Maynard* decision as well as several state court decisions, have given this view a judicial foothold. There seems to be a slightly more general acceptance that officers must obtain a Rule 41 warrant in order to compel a cell phone service provider to release prospective cell phone location information, but this requirement is by no means universal. With regard to historical cell phone location data, the majority position seems to be that a warrant is not required, although there is a determined minority of federal magistrate judges who, relying in part on the same logic that informed the *Maynard* decision, require a warrant in order to compel the release of records necessary for the prolonged tracking of a subscriber's movements.

Let us for a moment forget precedent and the current state of the *Katz* test for determining when a search has occurred. It seems likely enough that, if we focus on the broader principles contained in the Fourth Amendment—that officers of the government cannot be given broad discretion to interfere in the lives of citizens, even if they suspect them of lawbreaking—the Amendment would demand that the use of location tracking technology be considered a search. This technology makes it possible for the government to insinuate its investigative tentacles into the intimate and everyday portions of a people's lives in such a constant and broad manner that it would inarguably have troubled the authors of the Constitution, one of the main purposes of which was to check the powers of the government in relation to the individual. Prolonged electronic tracking, and cell-phone tracking specifically, provides the government with the capability to compile records of the activities of individuals that are Stasi-esque in their scope, and their use indicates a

---

219. *Id.* at 1789.

very different relationship between the government and individual than was contemplated by the founders. Mass-surveillance aside, to be able to record an individual's movements for a month without even having to expend more than a single manpower hour or make a preliminary evidentiary showing to a judge in order to do so, as is currently the case with the use of GPS units, is a massive grant of discretionary power to the government official and is suspect in the light of the Amendment's history.[220] The rationale put forward in the *Maynard* decision and by several federal magistrate judges in CSLI cases manages to satisfy these broader Fourth Amendment principles while still operating within the current jurisprudential framework. But, if these decisions are widely adopted and prolonged tracking found to be a search, would that be enough? Does a judicial or legislative determination that prolonged electronic tracking is a search and requires a search warrant go far enough in limiting the government officer's discretion as the Fourth Amendment seems to demand?

Perhaps because the question of whether or not prolonged use of the tracking technologies requires a warrant under the Fourth Amendment and applicable statutes has not been answered convincingly, proponents of the warrant requirement for prolonged tracking have not yet reached the second-order issue of whether a search warrant, as currently conceived of, would provide adequate Fourth Amendment protections. Accepting the mosaic theory advanced in *Maynard* and adopted in recent historical CSLI cases, the prolonged use of tracking technologies opens vast tracts of an individual's private life to government officials. This is owing to the fact that a tracking device, whether a GPS unit or a cell phone, is a blunt tool—it will collect the data it is designed to collect without discrimination, making no allowance for whether a person is engaged in activities other than those that interest the investigator. Tracking a person for a prolonged period can reveal all manner of activity that the individual would have considered secret: not only that someone is regularly visiting a known drug market, but also that they are involved in a fringe religion or are part of an environmental protest group. As one federal magistrate judge has put it in the context of CSLI,

> there is a legitimate scope problem with using a cell phone as a tracking device. The probable cause affidavit for CSLI rarely suggests that every activity in the target's life is illegal activity, yet receipt of CSLI will permit the government to "follow" the phone user's movements 24 hours a day, 7 days a week, wherever they go, whatever they are doing.[221]

It would seem that, in order to uphold the Fourth Amendment principles of specificity and limited official discretion, as illustrated in the *Entick* affair, the

---

220. Indeed, the power to track a person over a long period of time does not just make the government privy to information about a person that that person does not want to share, but can also impact other Constitutional rights. Just the threat of tracking can have a chilling effect on behavior, serving to suppress political protest, driving it deeply underground and insulating the dominant party from dissent. This possibility is not the product of civil-libertarian paranoia. In its report on domestic intelligence activities and the rights of Americans, the Church Committee observed that "[t]he Government has often undertaken the secret surveillance of citizens on the basis of their political beliefs, even when those beliefs posed no threat of violence or illegal acts on behalf of a hostile foreign power." Church Committee, *supra* note 8, at section C.

221. In re Application of U.S. for an Order (*Austin I*), 727 F. Supp. 2d 571, 582 (W.D. Tex. 2010).

process by which government officials are able to gain location information about a person should be tailored to provide as little information that is unrelated to the potential crime in question as possible. A failure to place such procedural limitations on electronic tracking would run the risk of warrants being issued that would function as general warrants: allowing for the collection of large volumes of unspecified information whether it was relevant to the investigation at hand or not.

A. The Current Warrant Options

1. The Standard Search Warrant

The standard search warrant, based as it is on the language of the Fourth Amendment, is designed to apply to situations where the government is trying to find physical property or evidence.[222] A list of the typical grounds for which a warrant may issue includes:

> (1) evidence of a crime;
> (2) contraband, fruits of crime, or other items illegally possessed;
> (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.[223]

In order for a warrant to issue, an affidavit establishing the grounds for issuing the warrant and specifying the person or place to be searched must be sworn to before the issuing judge.[224] The judge will then make a determination as to whether there is probable cause to believe that the grounds for issuance exists: that there has been a crime and that the search at issue will lead to recovery of the specified evidence, contraband or property that has been used in the crime.[225]

Referent as it is to physical evidence, the standard search warrant procedure does not create a framework that is readily adaptable to prolonged electronic tracking. Specifically, it does not provide any mechanism for dealing with the ongoing nature of the search and the fact that, by tracking a suspect over a prolonged period of time, the officers will necessarily be obtaining information beyond the specific information sought. More fundamentally, there is the question of what, exactly, is the "place to be searched"?

Traditional search warrants create an unclear time frame for how tracking would proceed. A federal search warrant requires that a warrant be executed within 14 days of issuance,[226] but what this would mean in the context of electronic tracking is not entirely clear. In the case of real-time tracking to be conducted in the future, such as a request for prospective CSLI or the use of a GPS unit, would execution encompass only the request for data from the cell service provider and the installation of the device, or would it also encompass the actual time period of the tracking? In requests for historical CSLI, would the execution of a warrant

---

222. *See* Orin S. Kerr, *Search Warrants in an Era of Digital Evidence*, 75 MISS. L.J. 85, 86 (2005) ("The existing law governing the warrant process presumes one-step searches common to the collection of traditional physical evidence.").

223. FED. R. CRIM. P. 41(c).

224. FED. R. CRIM. P. 41(e)(2)(A).

225. FED. R. CRIM. P. 41(d)(1).

226. FED. R. CRIM. P. 41(e)(2)(A)(i).

apply only to the request for the information, thus allowing a request for information from a length of time limited only by the duration of the suspect's cell phone account and the government's ability to make a case that the information would include relevant evidence? This would open huge amounts of information about a person to government eyes, defeating the principles of specificity and limited discretion contained in the Fourth Amendment.

2. The Current Federal Tracking Device Warrant

In 2006, the Federal Rules of Criminal Procedure were amended to include specific provisions relating to warrants for tracking devices.[227] These amendments go some way in clearing up the difficulties in applying the standard warrant requirements to the use of tracking devices.[228] They provide that federal magistrate judges must, upon a finding that there is probable cause that a grounds for issuance exists, issue a warrant for the installation and use of a tracking device.[229] The warrant itself must specify the person to be tracked and specify a reasonable time that the device can be used, with a maximum limit of 45 days subject to extension on a showing of good cause.[230] Furthermore, the amendments require that the officer obtaining the warrant must note the exact time of installation, as well as the period during which it was used.[231] The officer must also serve a copy of the warrant on the person who was tracked within 10 days of the date on which the tracking ended, although the government may request that notice be delayed if authorized by statute.[232]

While these requirements more clearly meet the challenge of providing a procedural framework that fits the context of electronic tracking—specifically in accounting for the fact that tracking is an ongoing process as opposed to a traditional physical search—they do not necessarily provide the maximum assurance possible that the information obtained through tracking will be adequately specific and that it will sufficiently limit the discretion of government officers. Most problematic in this sense is the allowance for tracking a person up to 45 days (or beyond, if an extension is granted). As noted above, it is likely impossible to utilize a tracking device in such a way that it records only information that there is probable cause to believe will be evidence of a crime or will lead to evidence of a crime.[233] The scope of the information obtained will always be greater than what is allegedly sought. If the goal is to allow government officers to use tracking information in order to obtain specified evidence (or

---

227. FED. R. CRIM. P. 41 advisory committee notes (2006 amendments).

228. The rule refers to the definition of "tracking device" contained in 18 U.S.C. § 3117(b). *See supra* note 184.

229. FED. R. CRIM. P. 41(d)(1). As noted above, the Federal Rules of Criminal Procedure do not require that a warrant be issued in order to use a tracking device, but only require that a magistrate judge issue a warrant for the installation and use of a tracking device upon the requisite showing.

230. FED. R. CRIM. P. 41(e)(2)(C).

231. FED. R. CRIM. P. 41(f)(2)(A).

232. FED. R. CRIM. P. 41(f)(2)(C), (f)(3).

233. Whether, under Rule 41, a tracking device can only be used where it itself records evidence of a crime or, on the other hand, will lead to evidence of a crime is up for debate. *See Austin I*, 727 F. Supp. 2d at 581-84 (discussing this issue in relation to CSLI).

specified data that will lead to evidence) but at the same time restrict, to the highest degree possible, extraneous information, a potentially 45-plus day tracking period without judicial oversight is too broad. It is too broad because, simply, it does not create enough of a procedural burden to the government to balance the fact that the government will be able to access much more information than it will actually need. Setting a default rule requiring more judicial oversight by decreasing the length of time that tracking could continue without reauthorization would encourage government officers to seek highly specified information (i.e. not engage in fishing expeditions) and to go about obtaining it in the most efficient way, thus limiting as much as possible their access to information unrelated to what they are seeking. Although the current rule can clearly be used by magistrate judges to this effect, it also allows for the possibility that magistrate judges sympathetic to the government can allow for long tracking periods in situations where the evidence provided in the government affidavit might not merit extended tracking.

Moreover, the current wording of the rule leaves some doubt about the treatment of cell-phone tracking. As federal magistrate judges have noticed, the definition of tracking device is so broad that when cell phone location information is sought to such a degree that it allows tracking, it is difficult to argue that a cell phone does not qualify as a tracking device.[234] However, the current tracking device warrant requirements technically leaves the issue open to debate, allowing for the potential of a massive gap in the regulation of electronic tracking by the government.

B. Suggestions for an Electronic Tracking Warrant

As discussed above, the current warrant requirements, whether under traditional search warrants or under the Federal tracking device warrant, may not provide the most effective protection from the government's ability to access information to which it is not entitled under the Fourth Amendment. What follows are several general suggestions for state rules committees, the Federal Rules Committee, or, alternatively, Congress, to consider in crafting electronic tracking warrants that will provide the most protection for citizens while still allowing the government to use electronic tracking in beneficial ways.[235] Several of these

---

234. *Id.* at 578 (quoting *Smith I*, 396 F. Supp. 2d at 753, and noting the breadth of the statutory definition of "tracking device").

235. Although these suggestions are aimed at both state and federal rules committees, the Federal Rules Committee indicates that only Federal Courts should issue warrants for the use of tracking devices. According to the Advisory Committee:

> Because the authorized tracking may involve more than one district or state, the Committee believes that only federal judicial officers should be authorized to issue this type of warrant. Even where officers have no reason to believe initially that a person or property will move outside the district of issuance, issuing a warrant to authorize tracking both inside and outside the district avoids the necessity of obtaining multiple warrants if the property or person later crosses district or state lines.

FED. R. CRIM. P. 41 advisory committee notes (2006 amendments). Despite this, several states currently provide for court orders authorizing the use of tracking devices. *See* 18 PA. CONS. STAT. § 5761 (2010) (authorizing the use of tracking devices on a showing of reasonable suspicion); UTAH CODE ANN. § 17-23a-15.5 (West 2010) (authorizing the use of tracking devices on a showing of relevancy to an ongoing

suggestions are informed by language from the Amended Wiretap Act,[236] which, although statutory, represents another instance in which decision makers have tried to create adequate safeguards for a surveillance technology that has the capacity to capture a much broader amount of information than is relevant to a specific investigation.[237]

Affidavits in support of a requested tracking warrant should include a "particular statement" of the information sought through tracking. This should include either the specific location(s) that a suspect is suspected of visiting (or not visiting), or else the nature of an unidentified location that the government is trying to identify, and the available evidence that indicates that the suspect's presence these locations constitutes evidence of a crime or will lead directly to evidence of a crime. Although this requirement may be considered inherent in the showing of probable cause, a clear statement of the expectation sets a tone of exacting specificity.

Likewise, affidavits in support of a request for a tracking warrant should include a statement laying out the evidence indicating that use of a tracking device *at the present time* will yield the information sought. Thus, to issue a tracking warrant, a judge will have to find that, not only is there probable cause to believe that a crime has been committed and that tracking will lead to the specified evidence of the crime, but also that there is probable cause that tracking during the specified period will lead to this evidence.

A rule creating a tracking device warrant should include language that specifically includes requests for cell phone location information when such requests have risen to the level of a search under the Fourth Amendment. Requests for cell phone records should be governed by the same requirements that would apply to a GPS tracking device because, as discussed above, cell phone tracking presents an even more invasive form of tracking. Moreover, since there is little difference between them in terms of the potential for the government to discover information not directly relevant to its investigation, the same requirements that apply to prospective tracking information should apply to requests for historical tracking. This leaves to the courts or Congress the determination of when a request for cell phone location rises to the level of a search.

Finally, and perhaps most controversially, the judge issuing the order should have the discretion to set a time limit on the tracking period, but no tracking should go on for longer than three weeks (21 days) without reauthorization from the

---

criminal investigation); OKLA. STAT. tit. 13, § 177.6 (2010) (allowing for the issuance of a warrant for the use of a tracking device on a showing of probable cause, but not requiring a warrant except where one is needed under the U.S. Constitution).

236. 18 U.S.C.A. § 2518 (West 2010). *See also supra* section IV.C.1.

237. Another iteration of this problem is found in police searches of computer hard drives. There, the problem is supplying the requisite specificity to conduct a search in which irrelevant files are not also opened and examined. In some cases, magistrate judges have felt the need to add further conditions and instructions to search warrants for hard drives. In 2009, the Federal Rules of Criminal Procedure were updated to recognize the two-step process that was necessary with computer searches. For a detailed overview of this issue, see Kerr, *supra* note 222; Orin S. Kerr, *Ex Ante Regulation of Computer Search and Seizure*, 96 VA. L. REV. 1241 (2010); Lily R. Robinton, *Courting Chaos: Conflicting Guidance From Courts Highlights the Need For Clearer Rules to Govern the Search and Seizure of Digital Evidence*, 12 YALE J. L. & TECH. 311 (2010).

issuing judge. The judge can reauthorize tracking upon either a showing of the results of the tracking period allowed to that point, or else a reasonable explanation of a failure to obtain the expected results, as well as a showing of good cause to believe that a reauthorization would further the investigative goals specified in the initial affidavit. The 21-day limit is, admittedly, a relatively arbitrary line. However, it is an attempt to balance the need for law enforcement officers to have adequate time to collect the information they seek with the need for sufficient oversight to protect citizens from unfocused investigations that dredge up more information than they ought to. As such, the 21-day limit strikes a reasonable balance, and the nature of the showing required for reauthorization should not overburden issuing judges.

These suggestions represent relatively minor tweaks to the current Federal tracking warrant requirements. However, they create a slightly more burdensome procedure for the government, a procedure designed to ensure that the government's use of tracking technology is narrowly focused on specified, judicially sanctioned ends.

VI. CONCLUSION

This Comment has attempted to map the legal landscape in relation to electronic tracking and to give a sense of the ongoing attempts that are being made to fit what for many is a visceral feeling—that warrantless location tracking is somehow violative of a fundamentally American relationship between the individual and the state—into the framework of the Supreme Court's Fourth Amendment Jurisprudence. It has also suggested that, should the Supreme Court find electronic tracking, or some forms of it, to be a search, a specific warrant with more safeguards than traditional search warrants and the current federal tracking warrant will be needed in order to provide sufficient protection from government overreach, whether accidental or purposeful.

In the coming term, the Supreme Court will weigh in on this issue. When they do, let us hope that as they look again at their precedent, they do so with one eye on the basic notions of specificity and limited discretion underlying the Fourth Amendment. As the Court itself said in *Boyd v. United States*, in reference to Lord Camden's decision in *Entick*:

> The principles laid down in [*Entick*] affect the very essence of constitutional liberty and security. They reach farther than the concrete form of the case then before the court . . . they apply to all invasions on the part of the government and its employ[ees] of the sanctity of a man's home and the privacies of life. It is not the breaking of his doors, and the rummaging of his drawers, that constitutes the essence of the offense; but it is the invasion of his indefeasible right of personal security, personal liberty and private property, where that right has never been forfeited by his conviction of some public offense,—it is the invasion of this sacred right which underlies and constitutes the essence of Lord Camden's judgment.[238]

238. 116 U.S. 616, 630 (1886).

Its decision in *United States v. Jones* will be another opportunity for the Court to realign its Fourth Amendment jurisprudence with the technology employed by government agents in order to safeguard the "privacies of life." However, even if it finds that prolonged electronic tracking is a search under the Fourth Amendment, protecting "personal liberty" and "personal security" demands that the Court, or Congress in its stead, must do the work of tailoring further procedure to prevent the "unjustifiable intrusion by the Government upon the privacy of the individual."[239]

239. Olmstead v. United States, 277 U.S. 438, 478 (1928) (Brandeis, J., dissenting).