Fordham Urban Law Journal

Volume 38, *Number* 2 2010 *Article* 5

THE CHALLENGE OF URBAN POLICING

BACK TO KATZ: REASONABLE EXPECTATION OF PRIVACY IN THE FACEBOOK AGE

Haley Plourde-Cole*

*

BACK TO KATZ: REASONABLE EXPECTATION OF PRIVACY IN THE FACEBOOK AGE

Haley Plourde-Cole

Abstract

Part I of this Note discusses the evolution of Fourth Amendment jurisprudence in reaction to advancing technology, the Supreme Court and circuit courts' disposition in dealing with electronic "beeper" tracking (the technology that predated GPS), and the legal doctrine governing the government's use of cellular phones to conduct surveillance of individuals both retroactively and in real-time. Part II examines the developing split among the federal circuits and state courts over whether GPS surveillance of vehicles constitutes a search, as well as the parallel concerns raised in recent published opinions by magistrate judges as to whether government requests for cell-site information from third party service providers require a warrant. Part III of this Note argues for the adoption of a rule that GPS surveillance constitutes a search and seizure and should require a warrant because the privacy expectation—that the government is not tracking its citizens twenty-four hours per day—is still one that society considers legitimate. It also argues that increasing public use or consent to third party use of GPS technology does not destroy an individual's reasonable expectation of privacy in his movements, nor indicate that society no longer views these expectations as reasonable. In fact, increased public awareness of recent technological invasions of privacy may be producing an increased demand for control over information.

KEYWORDS: GPS, surveillance, 4th Amendment, Katz

BACK TO *KATZ*: REASONABLE EXPECTATION OF PRIVACY IN THE FACEBOOK AGE

Haley Plourde-Cole[*]

[*] Fordham University School of Law, J.D. Candidate, 2012. My many thanks to Professor Andrew Kent for his invaluable feedback and commentary throughout this process, to Professor Mary Anne Wirth for introducing me to the case law that is the subject of this Note, and to the Editors and Staff of the *Fordham Urban Law Journal* for their hard work and dedication.

INTRODUCTION

On October 3, 2010, during a routine trip to the auto repair shop, a California student discovered a strange device attached to the back of his Ford Lincoln LS Sedan near the exhaust pipe.[1] The mechanic removed the device and later that day the student's friend posted photographs of it on the popular website Reddit.com, asking users, "[d]oes this mean the FBI is after us?"[2] His post continued, "[I] am pretty confident it is a tracking device by the FBI but my friend's roommates think it is a bomb . . . any thoughts?" [3] The Reddit.com users' responses suggested that it was indeed a tracking device—specifically, a Global Positioning System (GPS) device called the Guardian ST820, manufactured for law enforcement and military

1. Kim Zetter, *Caught Spying on Student, FBI Demands GPS Tracker Back*, WIRED.COM (Oct. 7, 2010, 10:13 PM), http://www.wired.com/threatlevel/2010/10/fbi-tracking-device/all/1.

2. Khaledthegypsy, *Does This Mean the FBI is After us?*, REDDIT.COM (Oct. 3, 2010), http://www.reddit.com/r/reddit.com/comments/dmh5s/does_this_mean_the_fbi_is_after_us.

3. *Id.*

use only by a company called Cobham.[4] Surely enough, the FBI showed up at the student's door just two days later asking for their device back.[5] The student obliged and the agents asked him several questions, indicating during the conversation that they had been tracking him for three to six months.[6] In the end, they let him go with a handshake. No need to call your lawyer, they reassured him: "Don't worry, you're boring."[7]

Meanwhile, the users of Reddit.com reacted with a mix of surprise and disgust at the student's discovery of a tracking device on his car. "Is it legal for the police/FBI to track anyone they feel like in the U.S.?"[8] "That's more than a little terrifying."[9] "This is officially the most insane thing I've ever seen on Reddit."[10] As a matter of fact, several months earlier the Ninth Circuit Court of Appeals held that law enforcement could attach such a device to a car while it was parked in a driveway and monitor it for several months without a warrant.[11] The issue has yet to come before the United States Supreme Court, although the Court addressed a different type of tracking in *United States v. Knotts*, in which it held that the government could monitor an electronic "beeper" placed in a can of chemicals to track a suspect on public roads without first obtaining a warrant.[12] In weighing the various policy implications of its ruling, however, the Court noted that "different principles may be applicable" when twenty-four hour surveillance or other "drag-net" law enforcement practices were possible.[13] Twenty-six years later, the proverbial Greek chorus of the legal community has spoken: "this time has come."[14]

4. Jeanmarcp, Comment to *Does This Mean the FBI is After us?*, REDDIT.COM (Oct. 3, 2010), http://www.reddit.com/r/reddit.com/comments/dmh5s/does_this_mean_the_fbi_is_after_us/c11bqxv.

5. *See* Zetter, *supra* note 1.

6. *Id.*

7. *Id.*

8. Alfadark, Comment to *Does This Mean the FBI is After us?*, REDDIT.COM (Oct. 3, 2010), http://www.reddit.com/r/reddit.com/comments/dmh5s/does_this_mean_the_fbi_is_after_us/c11bvvx.

9. *Id.*

10. TinManRC, Comment to *Does This Mean the FBI is After us?*, REDDIT.COM (Oct. 3, 2010), http://www.reddit.com/r/reddit.com/comments/dmh5s/does_this_mean_the_fbi_is_after_us/c11bgzy.

11. United States v. Pineda-Moreno, 591 F.3d 1212 (9th Cir. 2010), *reh'g denied*, 617 F.3d 1120.

12. 460 U.S. 276 (1983).

13. *Id.* at 283-84.

14. Recent Development, *Who Knows Where You've Been? Privacy Concerns Regarding the Use of Cellular Phones as Personal Locators*, 18 HARV. J.L. & TECH. 307, 317 (2004); *see also* United States v. Pineda-Moreno, 617 F.3d 1120, 1121 (9th Cir. 2010) (Kozinski, C.J., dissenting) ("1984 may have come a bit later than predicted, but it's here at last."); United States v. Garcia, 474 F.3d 994, 998 (7th Cir. 2007) (conceding that GPS

In fact, the government now has several ways to conduct twenty-four hour surveillance of virtually every citizen in this country, provided they drive a car or use a cell phone.[15] In the first instance, the government can attach a Global Positioning System device to a suspect's car and monitor his movements for an unlimited amount of time—with or without a warrant, depending on the jurisdiction.[16] Developed by the United States Department of Defense in the 1970s, the Navigational Satellite Timing and Ranging Global Positioning System (GPS) allows a receiver on earth to communicate with satellites that circle the earth on six orbital paths, and can typically calculate location within two meters.[17] GPS devices can be smaller than three inches wide, attached to objects such as vehicles, airplanes, and containers, and outfitted with wireless transmitters for remote monitoring.[18] Once attached to the suspect's vehicle, the device operates constantly, recording the vehicle's location at all hours and transmitting the information to law enforcement computers.[19]

In the second instance, the government may access similar information by compelling disclosure of location data from a cell phone service provider through a court order or a search warrant.[20] Cell phones are now able to provide even more precise twenty-four hour surveillance of citizens than are vehicles, given that a cell phone stays with an individual at nearly all times.[21] However, a cell phone does not even require a GPS chip to provide twenty-four hour surveillance capabilities; rather, because cell phones use radio signals to communicate between the users' handsets and the tele-

technology "enable[s] . . . wholesale surveillance"); People v. Weaver, 909 N.E.2d 1195, 1200 (N.Y. 2009) ("To say that that day has arrived involves no melodrama.").

15. For the purposes of this Note, "twenty-four hour surveillance" will refer to the *capability* of a GPS device or a cell phone to enable twenty-four hour surveillance, as opposed to the actual duration of surveillance or the degree of use of data from the devices. In the case of a GPS device attached to a suspect's car, the device operates constantly, providing twenty-four hour, real-time surveillance by remote monitoring. *See infra* notes 17-19 and accompanying text. In the case of cell phone surveillance, the government may request a court order for cell phone location data either prospectively, or retroactively, for unlimited periods of time. *See infra* notes 20-22 and accompanying text. The concept of twenty-four hour visual surveillance is addressed and distinguished in Part III.C.1.ii.

16. *See infra* Part II.

17. Renee McDonald Hutchins, *Tied up in* Knotts*? GPS Technology and the Fourth Amendment*, 55 UCLA L. REV. 409, 414-17 (2007).

18. *Id.* at 418-19.

19. *Id.* at 413, 418-19.

20. *See generally ECPA Reform and the Revolution in Location Based Technologies and Services: Hearing Before the Subcomm. on the Constitution, Civil Rights, and Civil Liberties of the H. Comm. on the Judiciary*, 111th Cong. 17-30 (2010) [hereinafter *ECPA Hearing*] (statement of Prof. Matthew A. Blaze), *available at* http://judiciary.house.gov/hearings/printers/111th/111-109_57082.PDF.

21. *See id.* at 19.

phone network, the network can calculate the location of active phones at any time, without any user action.[22] Although both methods of surveillance access similar information and are similarly intrusive, they have yet to receive much parallel legal analysis in either scholarship or judicial opinions. This is most likely due to the fact that cell phone information is governed by numerous federal statutes and the "Third Party Doctrine,"[23] whereas GPS surveillance of vehicles has no statutes on point and remains undecided by the nation's highest court. Recently however, several judges have begun to draw parallels between these types of government actions due to the similarities of the privacy interests at stake.[24]

The question of whether the Fourth Amendment's warrant requirement applies to these types of government actions is governed in part by the "*Katz* test," which asks whether the individual has a "reasonable expectation of privacy" in the area being searched.[25] Complicating the issue of government surveillance is the increased public use of this type of technology and the ever-increasing exposure of personal information to third parties. Many vehicles are sold with GPS devices, such as OnStar, already installed.[26] The cell phone is now a portable computer, outfitted with email, music players, Internet, and GPS technology.[27] In the latest "Smartphones," GPS location features are used in a myriad of applications, such as street directions, mapping, finding local restaurants, and even locating

22. *Id.* at 22. In fact, Professor Blaze notes that as "cellular carriers roll out better location technologies in the course of their business, the location information sent to law enforcement . . . is becoming more and more precise." *Id.* at 29. "New and emerging cell location techniques can work indoors and in places not typically accessible to GPS receivers. . . . without unusual or overt intervention that might be detected by the subject. And the 'tracking device' is now a benign object already carried by the target—his or her cell phone." *Id.* at 30.

23. In Fourth Amendment case law, the Third Party Doctrine reasons that a person has no legitimate expectation of privacy in information voluntarily disclosed to third parties. *See* Orin Kerr, *The Case for the Third Party Doctrine*, 107 MICH. L. REV. 561, 563 (2009) (citing as an example *Smith v. Maryland*, 442 U.S. 735, 743-44 (1979), which held that an individual has no reasonable expectation of privacy in the numbers he dials from his telephone because he voluntarily conveyed that information to the telephone company).

24. *See infra* Part II.C.

25. *See* Katz v. United States, 389 U.S. 347, 360-61 (1967) (Harlan, J., concurring).

26. ONSTAR BY GM, http://www.onstar.com/web/portal/onstartechnology (last visited Jan. 7, 2011). OnStar is one example of several security and navigation services that utilize GPS technology. OnStar is included in over forty General Motors vehicle models and available for installation on most other vehicles through local electronics retailers. *See* Press Release, OnStar, OnStar Expands Beyond GM Cars (Jan. 5, 2011), *available at* http://media.gm.com/content/product/public/us/en/onstar/news.detail.html/content/Pages/news/us/en/2011/Jan/0104_onstar.

27. *See ECPA Hearing*, *supra* note 20, at 19 (statement of Prof. Matthew A. Blaze).

other cell phone users.[28] The popular mobile telephone application "foursquare" permits users to affirmatively broadcast their location by "checking in" at a given location, such as a bar or restaurant, and share their location with friends and other users of the service.[29] Other applications like "Google Latitude" and Facebook's "Places" similarly allow users to share their location with friends.[30] Meanwhile, in other types of privacy encroachments, Google's email service "Gmail" searches its users' message content to determine which advertisements will appear on the sidebar of a user's inbox.[31] Most recently, Google has taken on the task of recording images of street corners in every major city in the world for "Google Street View."[32]

This rapid expansion of interactive technology begs the question whether increasing public awareness and use of this kind of technology should affect the legal interpretation of an individual's "reasonable expectation of privacy" in Fourth Amendment jurisprudence. Should private companies' level of access to this type of information determine the bar at which "reasonableness" is set? In light of the burgeoning circuit split regarding whether GPS surveillance of vehicles constitutes a search and seizure in the wake of the District of Columbia Circuit Court's decision in *United States v. Maynard*,[33] this Note will examine this dynamic, including how legal decisions regarding twenty-four hour surveillance of vehicles can be informed in part by the jurisprudence and legislative action regarding twenty-four hour surveillance of cell phone location data. Furthermore, this Note will examine shifting ideas around an individual's reasonable expectation of privacy given the increased consent to private use of personal information through GPS devices on vehicles, cellular phones, and in conjunction with social networking sites.[34]

Part I of this Note will discuss the evolution of Fourth Amendment jurisprudence in reaction to advancing technology, the Supreme Court and circuit courts' disposition in dealing with electronic "beeper" tracking (the technology that predated GPS), and the legal doctrine governing the gov-

28. *Id.* at 21.

29. *See* FOURSQUARE, http://foursquare.com (last visited Jan. 6, 2011).

30. *See* FACEBOOK PLACES, http://www.facebook.com/places (last visited Jan. 6, 2011); GOOGLE LATITUDE, http://www.google.com/mobile/latitude (last visited Jan. 6, 2011).

31. *Ads in Gmail and Your Personal Data*, GMAIL, http://mail.google.com/support/bin/answer.py?hl=en&answer=6603 (last visited Jan. 10, 2011).

32. *Google Maps With Street View*, GOOGLE MAPS, http://maps.google.com/help/maps/streetview/index.html (last visited Jan. 10, 2011).

33. 615 F.3d 544 (D.C. Cir. 2010), *reh'g denied sub nom.* United States v. Jones, 625 F.3d 766, 767, *cert. denied*, Maynard v. United States, No. 10-7102, 2010 WL 4156203 (Nov. 29, 2010).

34. *See infra* Part III.C.

ernment's use of cellular phones to conduct surveillance of individuals both retroactively and in real-time.[35] Part II will examine the developing split among the federal circuits and state courts over whether GPS surveillance of vehicles constitutes a search, as well as the parallel concerns raised in recent published opinions by magistrate judges as to whether government requests for cell-site information from third party service providers require a warrant.[36] Part III of this Note will argue for the adoption of a rule that GPS surveillance constitutes a search and seizure and should require a warrant because the privacy expectation—that the government is not tracking its citizens twenty-four hours per day—is still one that society considers legitimate.[37] It will also argue that increasing public use or consent to third party use of GPS technology does not destroy an individual's reasonable expectation of privacy in his movements, nor indicate that society no longer views these expectations as reasonable.[38] In fact, increased public awareness of recent technological invasions of privacy may be producing an increased demand for control over information.[39]

I. GOVERNMENT SURVEILLANCE AND THE FOURTH AMENDMENT: AN INCONSISTENT HISTORY

A. The Evolution of the Fourth Amendment in the Face of Changing Technology

The history of the Fourth Amendment is steeped in American colonial resistance to abuses by British officials; specifically, general "writs of assistance" which permitted British officers to enter any dwelling to search for prohibited goods.[40] Thus, the text of the Amendment 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.[41]

The United States Supreme Court has interpreted the text of the Amendment to mean that "searches conducted outside the judicial process, without

35. *See infra* Part I.

36. *See infra* Part II.

37. *See infra* Part III.A-C.

38. *See infra* Part III.C.2.

39. *See infra* notes 404-413 and accompanying text.

40. Vivek Kothari, Autobots, Decepticons, and Panopticons: The Transformative Nature of GPS Technology and the Fourth Amendment 6 (June 29, 2009) (unpublished article), *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1427476.

41. U.S. CONST. AMEND. IV.

prior approval by a judge or magistrate" are per se unreasonable, subject to "a few specifically established and well-delineated exceptions."[42] If law enforcement violated a defendant's Fourth Amendment rights, the evidence garnered from the unreasonable search and seizure must be suppressed under the exclusionary rule.[43]

From a practical perspective, therefore, the Fourth Amendment essentially functions as a procedural requirement;[44] rather than prohibiting searches and seizures altogether, it requires that law enforcement obtain a warrant based on probable cause.[45] Accordingly, one of the concerns of the Court in its Fourth Amendment jurisprudence has been providing "a workable accommodation between the needs of law enforcement and the interests protected by the Fourth Amendment."[46] In general, the Court has noted that judicial oversight of government surveillance devices is necessary to prevent abuse by law enforcement by requiring them to "demonstrate in advance their justification for the desired search."[47] The Fourth Amendment "does not contemplate the executive officers of Government as neutral and disinterested magistrates"; rather, the historical judgment encapsulated by the Fourth Amendment is that unlimited discretion among those with investigatory and prosecutorial duties would produce pressure to "overlook potential invasions of privacy."[48]

Because of its historical basis in the protection of private property from government intrusion before the advent of the Internet, telephone, radio, or satellite technology, the Fourth Amendment originally functioned within

42. Katz v. United States, 389 U.S. 347, 357 (1967). These exceptions, which have developed over time, include search incident to lawful arrest, Draper v. United States, 358 U.S. 307, 314 (1959), consent, United States v. Matlock, 415 U.S. 164, 165 (1974), the plain view doctrine, Horton v. California, 496 U.S. 128 (1990), stop and frisk, Terry v. Ohio, 392 U.S. 1 (1968), the automobile exception, Carroll v. United States, 267 U.S. 132 (1925), and exigent circumstances, United States v. Smith, 797 F.2d 836, 840 (10th Cir. 1986).

43. *See* Weeks v. United States, 232 U.S. 383 (1914).

44. *See* Kothari, *supra* note 40, at 8.

45. Some commentators have noted that the Fourth Amendment does not explicitly state that warrants are required at all; however this doctrine has been enshrined in Supreme Court case law. *See* United States v. Garcia, 474 F.3d 994, 996 (7th Cir. 2007) ("The Fourth Amendment forbids unreasonable searches and seizures. There is nothing in the amendment's text to suggest that a warrant is required in order to make a search or seizure reasonable. All that the amendment says about warrants is that they must describe with particularity the object of the search or seizure and must be supported both by an oath or affirmation and by probable cause. . . . The Supreme Court, however, has created a presumption that a warrant is required, unless infeasible, for a search to be reasonable."). Those searches that are reasonable are not considered "searches" within the meaning of the Fourth Amendment. *See* Kothari, *supra* note 40, at 8 (citing Kyllo v. United States, 533 U.S. 27, 27 (2001)).

46. Oliver v. United States, 466 U.S. 170, 181 (1984).

47. United States v. Karo, 468 U.S. 705, 717 (1984).

48. United States v. U.S. Dist. Ct., 407 U.S. 297, 317 (1972).

the context of common law trespass violations.[49] In 1928, when it first encountered the issue of wiretapping in *Olmstead v. United States*,[50] the Court held that because there was "no entry of the houses or offices of the defendants," the government had not violated the Fourth Amendment.[51] The Court began to move away from delineating Fourth Amendment violations by trespass standards in the latter half of the twentieth century. In *United States v. Silverman*,[52] the government attached a microphone to the heating duct of an apartment building in order to eavesdrop on conversations in an apartment. In finding that the government had violated the Fourth Amendment, the Court held that a "technical trespass" was not necessary; rather, it suffices if there is "actual intrusion into a constitutionally protected area."[53]

1. Katz *and its Progeny: Defining Reasonable Expectations of Privacy*

In the modern era, the Fourth Amendment is governed by the so-called "reasonable expectation of privacy" test, which has generated a large amount of scholarship and received much criticism since its birth.[54] The Court first dictated the test in *Katz v. United States*, which again broached the issue of warrantless wiretapping.[55] In *Katz*, government agents used a wiretap to listen and record the defendant while he spoke on a telephone in

49. *Kyllo*, 533 U.S. at 31.

50. 277 U.S. 438 (1928), *overruled by* Katz v. United States, 389 U.S. 347 (1967), *and* Berger v. New York, 388 U.S. 41 (1967).

51. *Id.* at 464.

52. 365 U.S. 505 (1961).

53. *Id.* at 510-12 (internal quotation marks omitted).

54. *See* Akhil Reed Amar, *Fourth Amendment First Principles*, 107 HARV. L. REV. 757, 759 (1994) ("Fourth Amendment case law is a sinking ocean liner—rudderless and badly off course—yet most scholarship contents itself with rearranging the deck chairs."); Orin S. Kerr, *Four Models of Fourth Amendment Protection*, 60 STAN. L. REV. 503, 505 (2007) ("Among scholars, this state of affairs [in Fourth Amendment law] is widely considered an embarrassment."). *But see* Hutchins, *supra* note 17, at 413 ("[T]he Fourth Amendment . . . provides a meaningful check on law enforcement's use of [GPS] technology."); Kerr, *supra*, at 507 ("What at first looks like conceptual confusion turns out to be a much-needed range of approaches."). For a list of articles critiquing the Court's "reasonable expectations of privacy" test under the Fourth Amendment, see Afsheen John Radsan, *The Case for Stewart Over Harlan on 24/7 Physical Surveillance*, 88 TEX. L. REV. 1475, 1493-97 nn.123-39 (2010).

While this Note will examine different modes of analysis used by courts when interpreting the Fourth Amendment in cases of electronic surveillance, the primary purpose of this discussion is not to identify flaws in jurisprudential application of Fourth Amendment doctrine. Rather, this Note will suggest how existing case law and evolving social norms can be applied to specific instances of government action, while taking note of some of these critiques.

55. *Katz*, 389 U.S. at 347.

a public phone booth.[56] The Court overruled *Olmstead* to hold that the wiretap "violated the privacy upon which the defendant justifiably relied" and thus constituted a search and seizure.[57] Solidifying the shift away from a focus on trespassory invasions, the Court held that the Fourth Amendment "protects people, not places," and therefore what an individual "seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected."[58] In his concurrence, Justice Harlan iterated the case's most quoted sentences: in his view, the majority's test to determine whether a defendant had a "reasonable expectation of privacy" in a given area involved a two-step inquiry: (1) whether the individual "exhibited an actual (subjective) expectation of privacy"; and (2) whether that expectation is "one that society is prepared to recognize as reasonable."[59]

While it is Justice Harlan's concurrence that came to be viewed as the "*Katz* test," this portion of the opinion has also received criticism for being unworkable and circular.[60] Critics argue that, while the majority in *Katz* treated the privacy interest embodied in the Fourth Amendment as a rule about control of information, the concurrence's reiteration and addition of society's legitimization converted the test into a "murky two-part analysis" that is almost impossible to administer.[61] First, the phrasing of the first prong requires individuals to have "exhibited an actual (subjective) expectation of privacy."[62] For example, the defendant in *Katz* entered a telephone booth, "shut[] the door behind him" and "[paid] the toll."[63] However, in today's world of satellite technology and the Internet, "[p]eople keep information about themselves private all the time without 'exhibiting' that interest in any perceptible way."[64] Due partly to the fact that so much information does not exist in physical form, individuals may maintain an expectation of privacy in their conversations, emails, or other types of information, but display no conscious efforts to keep them private.[65]

The second, and arguably larger, criticism is that the second prong's supposedly objective inquiry—the question of whether society "recognizes" as reasonable a certain privacy right—is one that is objectively unans-

56. *Id.* at 348.

57. *Id.* at 353.

58. *Id.* at 351.

59. *Id.* at 361 (Harlan, J., concurring) (internal quotation marks omitted).

60. Jim Harper, *Reforming Fourth Amendment Privacy Doctrine*, 57 AM. U. L. REV. 1381, 1385-1403 (2008).

61. *Id.* at 1386.

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

63. *Id.*

64. Harper, *supra* note 60, at 1386.

65. *Id.* at 1387.

werable by judges, philosophers, or even sociologists.[66] Consequently, the inquiry is essentially circular: "Societal expectations are guided by judicial rulings, which are supposedly guided by societal expectations, which in turn are guided by judicial rulings, and so on."[67] The challenge of discerning an "objective" standard for whether a privacy expectation is reasonable is exacerbated by the rapid evolution of technology, where expectations are neither static nor easily discernable.[68] Thus, some have argued, Harlan's concurrence converted the Fourth Amendment's focus on reasonableness of government action and placed it instead on the reasonableness of individuals in their own privacy.[69]

Justice Harlan himself has since criticized the use of the *Katz* test, writing that the critical question in fact should be "whether under our system of government, as reflected in the Constitution, we should impose on our citizens the risks of the electronic listener or observer without at least the protection of a warrant requirement."[70] Nevertheless, the *Katz* test remains precedential in Fourth Amendment law. In 1983, the Supreme Court again applied the "reasonable expectation of privacy test" in *United States v. Knotts*,[71] in which the Court addressed law enforcement's use of electronic "beepers"—tracking devices that emit a radio signal which can be attached to an item and followed using a radio receiver.[72] In *Knotts*, police placed a beeper inside a chloroform container and used it to track the defendant as he drove along public roads to a secluded cabin.[73] Reversing the Court of Appeals, the Supreme Court held that monitoring the signal of the beeper was not a search or seizure under the Fourth Amendment because "[a] person travelling in an automobile on public thoroughfares has no reasonable expectation of privacy in his movements from one place to another."[74] The Court also found that beeper surveillance amounted principally to visual surveillance because it achieved the same results.[75] There was nothing in the Fourth Amendment, the Court reasoned, that prohibited law enforcement from "augmenting the sensory faculties bestowed upon them at birth with such enhancement as science and technology afforded them in this

66. *Id.*
67. *Id.* at 1392.
68. *Id.*
69. *Id.* at 1386.
70. United States v. White, 401 U.S. 745, 786 (1971) (Harlan, J., dissenting).
71. 460 U.S. 276 (1983).
72. *See* Kothari, *supra* note 40, at 11.
73. *Knotts*, 460 U.S. at 277.
74. *Id.* at 281.
75. *Id.* at 282.

case."[76] In response to the defendant's contention that its holding would allow "twenty-four hour surveillance . . . without judicial knowledge or supervision,"[77] the Court drew a hypothetical line: "[I]f such dragnet type law enforcement practices . . . should eventually occur," it posited, "different constitutional principles may be applicable."[78]

Because the defendant did not believe he had standing to challenge the installation of the beeper into the container of chemicals before it was sold to him, the Court did not address whether the implantation itself might have constituted a search or seizure.[79] In his concurrence, however, Justice Brennan wrote that it would have been a "much more difficult case if respondent had challenged . . . [the beeper's] original installation," because earlier Fourth Amendment cases indicated that "when the government does engage in physical intrusion of a constitutionally protected area in order to obtain information, that intrusion may constitute a violation of the Fourth Amendment."[80] At least, he noted, the Court of Appeals' disposition of the installation issue with *caveat emptor* was incorrect.[81]

The Court again addressed a beeper case the following year, but failed to fully resolve the installation issue. In *United States v. Karo*,[82] the Court held that the installation of a beeper into a can of chemicals was not a search or seizure where the owner of the can had consented to the installation before it was transferred to the defendant.[83] Despite applying the consent exception to a warrant, the Court still noted the potential for abuse in government surveillance and made its preference for warrants abundantly clear; requiring warrants, the Court reasoned, would have "the salutary effect of ensuring that use of beepers is not abused, by imposing upon agents the requirement that they demonstrate in advance their justification for the desired search."[84] Furthermore, the Court found the government's contention that beeper surveillance should not require a warrant to be "based upon its deprecation of the benefits and exaggeration of the difficulties associated with procurement of a warrant."[85] After all, "if truly exigent cir-

76. *Id.*

77. *Id.* at 283 (internal quotation marks omitted).

78. *Id.* at 284.

79. *Id.* at 279 n.**.

80. *Id.* at 286 (Brennan, J., concurring) (emphasis omitted) (citing Silverman v. United States, 365 U.S. 505 (1961)).

81. *Id.*

82. 468 U.S. 705 (1984).

83. *Id.* at 706.

84. *Id.* at 717.

85. *Id.*

cumstances exist no warrant is required under general Fourth Amendment principles."[86]

Justice Stevens argued in dissent that regardless of the consent issue, the government's attachment of a beeper constituted a seizure, which the Court has defined as "some meaningful interference with an individual's possessory interests in that property."[87] By attaching the tracking device to the can of chemicals, the government "usurped a part of a citizen's property—in this case a part of respondents' exclusionary rights," which attached as soon as the can was delivered.[88] The government "in the most fundamental sense was asserting 'dominion and control' over the property—the power to use the property for its own purposes."[89] "As a general matter," Justice Stevens continued, "the private citizen is entitled to assume, and in fact does assume, that his possessions are not infected with concealed electronic devices."[90]

Because the installation issue was not thoroughly resolved by the Court, the door was left open for lower courts to rule differently in circumstances not subject to the consent exception. Several circuit courts addressed this issue both before and after *Knotts*, with most coming down on the side that installation was neither a search nor a seizure.[91] For example, in 1999 the

86. *Id.* at 717-18.

87. *Id.* at 728, 730 (Stevens, J., concurring in part and dissenting in part) (quoting United States v. Jacobsen, 466 U.S. 109, 113 (1984)).

88. *Id.* at 730.

> The owner of property, of course, has a right to exclude from it all the world, including the Government, and a concomitant right to use it exclusively for his own purposes. When the Government attaches an electronic monitoring device to that property, it infringes that exclusionary right; in a fundamental sense it has converted the property to its own use.

Id. at 729.

89. *Id.* at 730 (quoting *Jacobsen*, 466 U.S. at 120).

90. *Id.* at 735.

91. These cases generally divide into three camps. The first camp held that attachment of a tracking device to a defendant's property did not constitute a search or seizure. *See, e.g.*, United States v. McIver, 186 F.3d 1119, 1126-27 (9th Cir. 1999) (holding that installation of beeper to defendant's car did not constitute a search or seizure where vehicle was outside the "curtilage" of defendant's residence); United States v. Pretzinger, 542 F.2d 517, 520 (9th Cir. 1976) (holding that installation of beeper on an airplane parked at a repair shop was not a search).

A second camp held that attachment of such a device did not require a warrant, but did require the existence of either probable cause or reasonable suspicion. *See, e.g.*, United States v. Michael, 645 F.2d 252, 258 (5th Cir. 1981) (holding that attachment of a beeper to defendant's van was justified where law enforcement had "reasonable suspicion" to attach the device); United States v. Shovea, 580 F.2d 1382, 1377 (10th Cir. 1978) (holding that installation of a beeper on car parked on a public street was not a search where federal agents had sufficient probable cause without first acquiring a court order); United States v. Moore, 562 F.2d 106, 113 (1st Cir. 1977) (holding that attachment of an electronic beeper to

Ninth Circuit held in *United States v. McIver*[92] that the attachment of a beeper to a vehicle parked in a driveway was not a "search" because the vehicle was parked "outside the curtilage" of the defendant's residence, was open to public view, and because the defendant did not show that he "intended to shield the undercarriage of his vehicle from inspection by others."[93] The court held that the installation of the device was not a seizure because the officers did not meaningfully interfere with the defendant's possessory interest in the vehicle.[94]

On the other hand, the Fifth Circuit, considering the issue prior to the Supreme Court's decision in *Knotts*, held that both the installation and monitoring of a tracking device constituted a search and seizure, and required a warrant.[95] In distinguishing the installation of a beeper from other actions validated by the Supreme Court, the Fifth Circuit found installing a tracking device constituted an ongoing invasion, akin to "hiding an agent in the trunk."[96] Furthermore, the "presence or absence of a physical intrusion into the interior of the car" was irrelevant to whether the installation was a search or seizure.[97] In considering the defendant's reasonable expectation of privacy, the court maintained that it was "unwilling to hold that Holmes, and every other citizen, runs the risk that the government will plant a bug in

the undercarriage of a van did not require a warrant where officers had probable cause to suspect a "criminal enterprise was underway"). It should be noted that this standard, which allows for an *ex post facto* determination of reasonable suspicion or probable cause seems to contradict directly the Supreme Court's statement in *Katz v. United States* that "this court has never sustained a search upon the sole ground that officers reasonably expected to find evidence of a particular crime. . . . Searches conducted without warrants have been held unlawful notwithstanding facts unquestionably showing probable cause." 389 U.S. 347, 356-57 (1967) (internal quotation marks omitted).

A third camp held that installation may constitute a search and seizure and require a warrant. In *United States v. Bruneau*, 594 F.2d 1190, 1194 (8th Cir. 1979), which addressed the attachment of a transponder to an airplane, the court held that the installation of the device could constitute a search or seizure, but found no violation in that case because it was attached with the consent of the owner. In *United States v. Holmes*, the Fifth Circuit held that both the installation and monitoring of a beeper violated the Fourth Amendment. 521 F.2d 859, 865 (5th Cir. 1975), *aff'd en banc*, 537 F.2d 227 (5th Cir. 1976).

92. 186 F.3d at 1119.

93. *Id.* at 1126-27. The curtilage has been defined as "the area to which extends the intimate activity associated with the 'sanctity of a man's home and the privacies of life' and therefore has been considered part of the home itself for Fourth Amendment purposes." Oliver v. United States, 466 U.S. 170, 180 (1984) (quoting Boyd v. United States, 116 U.S. 616, 630 (1886)).

94. *Id.*

95. *Holmes*, 521 F.2d at 872.

96. *Id.* at 865 n.11.

97. *Id.* at 865.

his car in order to track his movements, merely because he drives his car in areas accessible to the public."[98]

In 1986, the Supreme Court decided another case which marked the expansion of the government's ability to utilize modern technology. In *Dow Chemical Co. v. United States*, the Court held that the Environmental Protection Agency's (EPA) aerial photography of a chemical company's industrial complex did not constitute a search under the Fourth Amendment.[99] While noting that the government generally has greater latitude in conducting inspections of commercial property, the Court held that the defendants also had no reasonable expectation of privacy in the complex because the photographs did not reveal "intimate details"[100] of the structure; rather, the images were limited to the outline of the facility's buildings and equipment.[101] The defendant also lacked a reasonable expectation in the industrial complex because the EPA was using a conventional commercial camera widely available to the public, and because its "open areas" were comparable to an open field, which is generally not covered by the Fourth Amendment.[102] In a later case, the Court held in *Florida v. Riley* that police did not need a warrant to conduct surveillance of an individual's private property by helicopter because "no intimate details" of the property were revealed and the officers were flying legally in public airspace.[103]

The Supreme Court recently confronted another type of emerging technology in *Kyllo v. United States*.[104] There, law enforcement used a thermal-imaging device to detect relative amounts of heat within the defendant's home, from which they surmised the presence of heat lamps used for growing marijuana.[105] Reversing its trend of relative permissiveness towards new technologies,[106] Justice Scalia wrote for a 5-4 majority that the use of a thermal-imaging device was a search and seizure because "any information regarding the interior of the home that could not otherwise have been obtained without physical intrusion into a constitutionally protected

98. *Id.*

99. 476 U.S. 227, 227-28 (1986).

100. *Id.* at 228.

101. *Id.* at 238.

102. *Id.* at 236-39 (citing Oliver v. United States, 466 U.S. 170, 179 (1984)). Under the "Open Fields Doctrine," Fourth Amendment protection generally does not extend beyond the area immediately surrounding a private house because it does not "provide the setting for those intimate activities that the [Fourth] Amendment is intended to shelter from governmental interference or surveillance." *Id.* at 235-36 (alteration in original) (quoting *Oliver*, 466 U.S. at 179).

103. 488 U.S. 445, 446, 451 (1989).

104. 533 U.S. 27 (2001).

105. *Id.* at 27.

106. *See* Kothari, *supra* note 40, at 11.

area" constituted a search.[107] In addressing the issue of changing technology, the Court stated that, although it had previously reserved judgment as to how technological enhancement implicated the Fourth Amendment, "the rule we adopt must take account of more sophisticated systems that are already in use or in development."[108] Justice Scalia's opinion also discounted the dissent's point that the same information could have been obtained by conducting visual surveillance from the street:

> The fact that equivalent information could sometimes be obtained by other means does not make lawful the use of means that violate the Fourth Amendment. The police might, for example, learn how many people are in a particular house by setting up year-round surveillance; but that does not make breaking and entering to find out the same information lawful.[109]

2. Modes of Fourth Amendment Analysis

Thus, despite the arguably convoluted nature of the *Katz* test, the Court has generally considered several factors when approaching new technology, including the type of technology being employed, the quantity and quality of information being revealed, whether the technology is widely used by the public, and whether the action is otherwise legal.[110] However, the Court's weighing of these elements is not always consistent. For example, in *Knotts*, the Court found no search where law enforcement made "limited use" of signals from an electronic beeper, and where visual surveillance "would have sufficed to reveal all of these facts to the police."[111] Yet in *Kyllo*, where the technology was also "relatively crude," the heat-sensing technology was ruled a search because the information revealed "intimate details" of the home.[112] Furthermore, whereas the beeper in *Knotts* was held to be a mere substitute for visual surveillance,[113] the heat-detecting device in *Kyllo* was considered "sense-enhancing" and thus unconstitutional, at least where it was not in use by the general public.[114] On

107. *Kyllo*, 533 U.S. at 34 (citing Silverman v. United States, 365 U.S. 505, 512 (1961)). In Supreme Court jurisprudence, the search of a home is presumptively unreasonable. *See* Payton v. New York, 445 U.S. 573, 586 (1980).

108. *Kyllo*, 533 U.S. at 36.

109. *Id.* at 35 n.2.

110. *See* Kothari, *supra* note 40, at 10-12.

111. United States v. Knotts, 460 U.S. 276, 282, 284 (1983).

112. *Kyllo*, 533 U.S. at 31, 36 ("At 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." (internal quotation marks omitted)).

113. *Knotts*, 460 U.S. at 281-82.

114. *Kyllo*, 533 U.S. at 28.

the other hand, although a photographic camera is arguably sense-enhancing, the Court held that photographs of an industrial complex were not a search because it was a type of technology widely available to the public and revealed no intimate details.[115]

Additionally, Fourth Amendment jurisprudence can be understood through several modes of analysis which focus on the Court's underlying concerns.[116] These "models of Fourth Amendment protection" break down into four categories: (1) the probabilistic model, which considers the likelihood that the subject's information would become known to the general public or law enforcement, and thus informs whether the subject could have had a subjective expectation of privacy;[117] (2) the private facts model, which asks whether the government's conduct reveals particularly private and personal information deserving of protection;[118] (3) the positive law model, which considers whether the government conduct interferes with property rights or violates other laws outside the Fourth Amendment;[119] and (4) the policy model, which focuses on whether the police conduct at issue is one which the Court feels should be regulated by an impartial judicial magistrate.[120] These models are especially helpful in identifying priorities in cases involving GPS surveillance.

115. Dow Chemical Co. v. United States, 476 U.S. 227, 237-38 (1986); *see also supra* notes 99-102 and accompanying text.

116. *See* Kerr, supra note 54, at 503.

117. *See id.* at 508-12. One example of the Supreme Court utilizing the probabilistic approach is *Bond v. United States*, 529 U.S. 334 (2000). In *Bond*, the Court held that the squeezing of a bus passenger's luggage by a border patrol agent constituted a search because it exceeded the usual handling of luggage, and thus was contrary to the reasonable expectations of bus passengers. *Id.* at 337-39. In the same vein, the Court held in *California v. Ciraolo*, 476 U.S. 207, 215 (1986), that aerial surveillance did not violate a defendant's reasonable expectation of privacy because aerial observation was deemed common in the modern age. Although the dissent disagreed on the likelihood of observation by air, both the majority and dissenting opinions agreed that the proper inquiry included the likelihood that the suspect's property would be subject to observation by others. *Id.* at 223 (Powell, J., dissenting).

118. Kerr, *supra* note 54, at 512-14 (citing *Dow Chemical Co.*, 476 U.S. at 227, and *United States v. Karo*, 468 U.S. 705, 729-30 (1984), both of which focus on whether surveillance revealed "intimate details," or particularly personal or private information).

119. *Id.* at 516-19 (citing *Dow Chemical Co.*, 476 U.S. at 228, and Florida v. Riley, 488 U.S. 445 (1989)).

120. *Id.* at 519-22 (citing *Kyllo v. United States*, 533 U.S. 27, 34 (2001), noting that its holding "assures preservation of that degree of privacy against government that existed when the Fourth Amendment was adopted").

B. Cell Phones as Tracking Devices: The Implications of the Third Party Doctrine Under the Fourth Amendment

As mentioned above, the legal discussion of cell phones is somewhat removed from the tracking of vehicles because government use of communications information from these devices is governed in part by the Third Party Doctrine, which reasons that a person has no legitimate expectation of privacy in information voluntarily disclosed to third parties.[121] Over the past twenty-five years the cell phone has transformed into a portable computer, outfitted with email, music players, the Internet, and location applications which utilize GPS technology.[122] However, a cell phone does not even require a GPS chip for it to provide twenty-four hour surveillance capabilities; because cell phones use radio to communicate between the users' handsets and the telephone network, the network can calculate the location of active phones at any time, without any user action.[123] These rapidly advancing developments in cell phone technology have caused judges, from the magistrate level to the Court of Appeals for the Third Circuit, to analyze the use of this information under the reasonable expectation of privacy test articulated in *Katz*, with several explicitly referencing recent cases addressing GPS vehicle surveillance.[124]

To obtain access to this data, a government agent may appear before a magistrate judge and apply for a court order to compel the desired information from the third party service provider. A chief function of magistrate judges is to issue search warrants and other orders in aid of criminal investigations, including electronic surveillance orders for pen registers,[125] trap and trace devices,[126] tracking devices, and orders for telephone and email

121. *See* Smith v. Maryland, 442 U.S. 735, 742-44 (1979) (holding that an individual has no reasonable expectation of privacy in the numbers he dials from his telephone because he voluntarily conveyed that information to the telephone company). This premise has also been extended to email recipients and Internet website addresses. *See* United States v. Forrester, 512 F.3d 500, 510 (9th Cir. 2008) ("[E]-mail and Internet users have no expectation of privacy in the to/from addresses of their messages or the IP addresses of the websites they visit because they should know that this information is provided to and used by Internet service providers for the specific purpose of directing the routing of information.").

122. *See supra* notes 29-30 and accompanying text.

123. *ECPA Hearing*, *supra* note 20, at 22 (statement of Prof. Matthew A. Blaze); *see also supra* text accompanying note 22.

124. See *infra* Part II.C.2.

125. A pen register is an electronic device that records all numbers dialed from a particular telephone line. *See* Smith v. Maryland, 442 U.S. 735, 735 (1979).

126. A trap and trace device records all transmissions from a telecommunications system, including both incoming and outgoing phone numbers, and other dialing, routing, addressing, and signaling information likely to identify the source of a wire or electronic communication. *See* 18 U.S.C. § 3127(3) (2006).

account records.[127] The increasing popularity of cell phones in 1986 prompted the U.S. Congress to enact the Electronic Communications Privacy Act (ECPA),[128] which authorized various criminal investigative tools under four different legal standards: pen registers and trap/trace devices have the least demanding standard (the information sought must be "relevant to an ongoing investigation"),[129] stored communications and account records are accessible with "specific and articulable facts,"[130] tracking device warrants are covered by the Rule 41 "probable cause" standard,[131] and wiretap orders have a "super-warrant" requirement.[132] According to some estimates, the total number of electronic surveillance orders issued at the federal level each year substantially exceeds 10,000.[133]

One problem for courts in regulating cell phone tracking information disclosure is that "the ECPA doesn't explicitly refer to 'cell site' or other location information from a cell phone."[134] Thus, where government officials seek to compel cell phone tracking information on a prospective basis, some magistrates have used the probable cause standard for a "tracking device,"[135] defined in the ECPA as "an electronic or mechanical device which permits the tracking of the movement of a person or object."[136]

Thus, the emerging case law regarding whether cell-site location data requires a warrant is useful to inform the larger question of whether twenty-four hour surveillance in all its forms should be subject to the warrant

127. *ECPA Hearing*, *supra* note 20, at 79 (statement of Stephen Wm. Smith, U.S. Mag. J.).

128. Pub. L. No. 99-508, 100 Stat. 1848 (1986) (codified as amended in scattered sections of 18 U.S.C.).

129. *ECPA Hearing*, *supra* note 20, at 82 (statement of Stephen Wm. Smith, U.S. Mag. J.); *see also* 18 U.S.C. § 3122 (2006).

130. *ECPA Hearing*, *supra* note 20, at 82 (statement of Stephen Wm. Smith, U.S. Mag. J.) (citing 18 U.S.C. § 2703 (2006)).

131. *Id.* (citing 18 U.S.C. § 3117 (2006)); *see also* FED. R. CRIM. P. 41.

132. *ECPA Hearing*, *supra* note 20, at 82 (statement of Stephen Wm. Smith, U.S. Mag. J.). The warrant requirement for a wiretap is often called a "super-warrant" because it requires a higher standard of probable cause than an ordinary search warrant. *See* 18 U.S.C. § 2518(3) (2006); Samantha L. Martin, Note, *Interpreting the Wiretape Act: Applying Ordinary Rules of "Transit" to the Internet Context*, 28 CARDOZO L. REV. 443, 445 nn.28-29 (2006).

133. *ECPA Hearing*, *supra* note 20, at 80. During 2006, 15,177 criminal matters handled by magistrate judges in federal court were completely sealed from the public, and the "vast majority of those were warrant-related applications." *Id.* While "[t]he ECPA requires the Attorney General to report to Congress the number of pen registers applied for annually. . . . there is no separate reporting requirement for tracking devices under § 3117 or location information obtained under § 2703(d)." *Id.* at 80 n.2.

134. *Id.* at 82.

135. *See id.*

136. 18 U.S.C. § 3117(b) (2006).

requirements of the Fourth Amendment. A more detailed analysis of some of these decisions will appear in Part II of this Note.

II. "THE END OF PRIVACY"[137]—OR NOT?: THE EMERGING SPLIT OVER GOVERNMENT SURVEILLANCE

Twenty-six years after *Knotts*, the Supreme Court has yet to decide a case involving twenty-four hour GPS surveillance. This silence has left the lower courts to analogize between beeper and GPS technology, while attempting to heed the Court's cautionary words regarding twenty-four hour surveillance.[138] The result has been a split among both the federal circuit and state courts as to whether GPS surveillance should require a warrant based on probable cause.[139] Until recently, most of the federal circuits to hear the issue have hesitated to distinguish GPS technology from the beeper in *Knotts*, analogizing GPS surveillance to following a vehicle on public roads.[140] In 2010, the District of Columbia Court of Appeals became the first federal circuit to distinguish GPS surveillance from a beeper, holding that it constitutes a search under the Fourth Amendment.[141] Meanwhile, several state courts had reached a similar conclusion under their State Constitutions.[142] Part II of this Note will detail the varying modes of analysis at play on both sides of this burgeoning split.

A. Cases Holding GPS Surveillance Does Not Require a Warrant

1. Circuit Courts Finding No Search or Seizure

The Seventh Circuit was the first to expressly address both the installation and monitoring of a GPS device in 2007. In *United States v. Garcia*, police officers placed a GPS device under the rear bumper of the defendant's vehicle after hearing from two sources that he planned to manufacture crystal methamphetamine ("meth").[143] The officers learned from the GPS device that the defendant had driven the vehicle to a large tract of land, where they subsequently found the equipment and chemicals required to manufacture meth.[144] Relying on *Knotts*, Judge Richard Posner, writing

137. *See* John D. Sutter, *The Internet and the 'End of Privacy,'* CNN.COM (Dec. 13, 2010), http://articles.cnn.com/2010-12-13/tech/end.of.privacy.intro_1_online-privacy-blippy-social-network?_s=PM:TECH.

138. *See infra* Part II.A-B.

139. *See infra* Part II.A-B.

140. *See infra* Part II.A.

141. *See* United States v. Maynard, 615 F.3d 544, 555 (D.C. Cir. 2010).

142. *See infra* Part II.B.1.

143. 474 F.3d 994, 995 (7th Cir. 2007).

144. *Id.*

for the court, found that no "search" occurred in the installation or monitoring of the GPS device, because the technology substituted an activity (following a car on a public street) that was "unequivocally not a search."[145] Additionally, the court found that no "seizure" occurred at the time of installation because the device did not: (1) affect the vehicle's driving qualities; (2) draw power from the engine or battery; (3) take up room in the vehicle; or (4) alter the appearance of the vehicle.[146] Recognizing that GPS technology enabled "wholesale surveillance,"[147] the court conceded that one could "imagine the police affixing GPS tracking devices to thousands of cars at random, recovering the devices, and using digital search techniques to identify suspicious driving patterns."[148] However, it refrained from resolving the constitutionality of that scenario until it became apparent that a program of "mass surveillance" was in fact in effect.[149]

The Eighth Circuit also addressed the issue of GPS surveillance in *United States v. Marquez*.[150] In that case, law enforcement had attached a GPS device to a truck in which the defendant was occasionally a passenger and monitored it for several months.[151] They replaced the battery on the device on seven occasions, each time while the vehicle was parked on a public street.[152] Tracking the device remotely, the police discovered the truck had been traveling back and forth between Colorado and Iowa, leading them to uncover a large marijuana distribution ring.[153] While the court found that

145. *Id.* at 997-98. The Seventh Circuit's decision has later been analyzed as requiring "reasonable suspicion" for the attachment of a GPS device. *See* United States v. Marquez, 605 F.3d 604, 610 (8th Cir. 2010). However, it is unclear from the opinion that the court required any showing of cause; while the court noted that the District Court found the police had reasonable suspicion, *see Garcia*, 474 F.3d at 996, it did not explicitly require a standard for warrantless attachment of tracking devices. Rather, it focused on whether the police were conducting "mass surveillance"; because it appeared the police of Polk County were not engaged in that type of activity, the use of GPS surveillance without a warrant did not implicate the Fourth Amendment. *Id.* at 998.

146. *Garcia*, 474 F.3d at 996. While Judge Posner did not state from where he drew the rule for this particular seizure analysis, it is likely he was relying on the notion of seizure expressed in *United States v. Jacobsen*, which states that a "seizure" of property occurs "when there is some meaningful interference with an individual's possessory interests in that property." 466 U.S. 109, 113 (1984).

147. *Garcia*, 474 F.3d at 998.

148. *Id.*

149. *Id.*

150. *Marquez*, 605 F.3d at 604.

151. While the court does not explicitly state the length of the monitoring, it is clear from the government's brief that the GPS device was on the vehicle from at least May 2, 2007 to July 21, 2007, though it is possible GPS surveillance continued through October 2007. *See* Brief for Appellee at 6, 9, United States v. Marquez, 605 F.3d 604 (8th Cir. 2010) (No. 09-1743), 2009 WL 2955451.

152. *Marquez*, 605 F.3d at 607.

153. *Id.*

the defendant did not have standing to challenge the installation or use of the GPS device because he was not the owner of the vehicle, it held that even if he had, the surveillance did not violate the Fourth Amendment because the vehicle was traveling on public roads.[154] The Eighth Circuit also required, however, that law enforcement have "reasonably suspected" the vehicle was involved in a drug ring to justify the tracking device.[155] While noting that "wholesale surveillance" was entirely possible given the low-cost of GPS technology, the court wrote that because the government's action was not "random and arbitrary," no Fourth Amendment concerns were implicated.[156] The Eight Circuit's holding reflects similar earlier determinations by the First, Fifth, and Tenth Circuits that—while declining to require a warrant—there must be some intermediate level of cause to justify the use of a tracking device.[157]

The Ninth Circuit also recently addressed the use of GPS tracking by law enforcement in *United States v. Pineda-Moreno*.[158] There, Drug Enforcement Agency (DEA) officials monitored the defendant over a four-month period, attaching several mobile tracking devices (including a GPS device[159]) to his Jeep on seven different occasions.[160] On four occasions, DEA officials installed the devices—each about the size of a bar of soap—while the defendant's vehicle was parked on a public street in front of his home.[161] On two occasions, it was parked in his driveway, a few feet from his mobile home, and on one occasion, it was in a public parking lot.[162] Relying on *Knotts* and *Garcia*, the Ninth Circuit held that the monitoring of the GPS device did not amount to a search under the Fourth Amendment because the information obtained from the tracking devices could have also been obtained by visual surveillance, and thus the defendant had no reasonable expectation of privacy in his movements.[163] In so holding, the court rejected the defendant's claim that the Supreme Court had modified its

154. *Id.* at 609.

155. *Id.* at 610. In so holding, the court referred to the Seventh Circuit in *Garcia* for the proposition that police could install a "non-invasive" GPS tracking device for a "reasonable amount of time," where police had "reasonable suspicion" to do so. *Id.* However, it is unclear that *Garcia* actually required a finding of reasonable suspicion. *See supra* note 145.

156. *Id.*

157. *See supra* note 91.

158. 591 F.3d 1212 (9th Cir. 2010), *reh'g denied*, 617 F.3d 1120.

159. *See* Brief for Appellant at 12, United States v. Pineda-Moreno, 591 F.3d 1212 (9th Cir. 2010) (No. 8-30385).

160. *Pineda-Moreno*, 591 F.3d at 1213.

161. *Id.*

162. *Id.*

163. *Id.* at 1216.

Fourth Amendment analysis in *Kyllo v. United States*,[164] which held that a warrant was required to use a thermal-imaging device even where similar information could have been obtained by visual surveillance.[165] The Ninth Circuit found the case distinguishable because the thermal-imaging in *Kyllo* provided a substitute for action that constituted a search under the Fourth Amendment (information regarding the interior of a home), whereas a GPS device substituted for following a car on a public street, which was not a search.[166]

The court also held that the installation of the device was not a search because the defendant had no expectation of privacy in the undercarriage of his vehicle.[167] However, the Ninth Circuit went even further than the Seventh Circuit in *Garcia* or its own previous holding in *United States v. McIver*,[168] to hold that the defendant lacked a reasonable expectation of privacy even when his vehicle was parked in the driveway of his residence.[169] While acknowledging that the driveway has usually been considered part of the "curtilage" of the home (and thus a "protected space" in Fourth Amendment jurisprudence), the court found that it was still only a "semi-private area."[170] To demonstrate a reasonable expectation of privacy in his driveway, the court held, the defendant must "support that expectation by detailing the special features of the driveway itself (i.e., enclosures, barriers, lack of visibility from the street) or the nature of activities performed upon it."[171] Because the defendant had no gate around his driveway, no "No Trespassing" signs, and no "features to prevent someone standing in the street from seeing the entire driveway," the defendant had not demonstrated that he had taken any "steps to exclude passersby from his driveway," and thus could not claim a reasonable expectation of privacy.[172] Consequently, the Ninth Circuit's holding has been seen as an ex-

164. 533 U.S. 27 (2001).

165. *See Pineda-Moreno*, 591 F.3d at 1216 (discussing *Kyllo*, 533 U.S. at 34-35).

166. *See id.*

167. *Id.* at 1214.

168. 186 F.3d 1119, 1127 (9th Cir. 1999); *see also supra* notes 92-93 and accompanying text.

169. *Pineda-Moreno*, 591 F.3d at 1214-15.

170. *Id.* at 1215 (citing United States v. Magana, 512 F.2d 1169, 1171 (9th Cir. 1975)).

171. *Id.* (citing Maisano v. Welcher, 940 F.2d 499, 503 (9th Cir. 1991)).

172. *Id.* Pineda-Moreno's petition for a re-hearing en banc was denied in August of 2010. *See* United States v. Pineda-Moreno, 617 F.3d 1120 (9th Cir. 2010). Writing in dissent, Chief Judge Kozinski decried the panel's decision, most specifically to the point of whether Pineda-Moreno's driveway, as part of his curtilage, retained a heightened level of privacy. *Id.* at 1121 (Kozinski, C.J., dissenting). Arguing that it did not, the Chief Judge argued that the Ninth Circuit had disobeyed Supreme Court precedent, which defines the "curtilage" as the area associated with "the sanctity of a man's home and the privacies of life," and states explicitly that it "warrants the Fourth Amendment protections that attach to

pansion of the government's ability to conduct warrantless GPS surveillance.[173]

A recent case from the First Circuit—albeit in the District Court—is one of the first examples of a court including analysis of public use and knowledge of GPS tracking technology in its determination of an individual's reasonable expectation of privacy. In *United States v. Sparks*,[174] the FBI placed a GPS device on the defendant's black Chrysler while it was parked in the private parking lot of his apartment building because they believed he was responsible for three armed robberies in the preceding months.[175] Eleven days into the surveillance, the police used the GPS device to locate the defendant's car, and while conducting visual surveillance of the ve-

the home." *Id.* at 1121-22 (citing Oliver v. United States, 466 U.S. 170, 180 (1984)). Asking the defendant to separately establish a reasonable expectation of privacy in his "curtilage," the dissent wrote, "is like requiring the homeowner to establish a reasonable expectation of privacy in his bedroom." *Id.* at 1122.

Moreover, the dissent worried that the panel's rationale for concluding Pineda-Moreno had no reasonable expectation of privacy in his driveway would affect future defendants inconsistently; based on the panel's decision, those who could afford to protect their privacy "with the aid of electric gates, tall fences, security booths, remote cameras, motion sensors and roving patrols," would be protected by the Fourth Amendment, where "the vast majority of the 60 million people living in the Ninth Circuit will see their privacy materially diminished by the panel's ruling." *Id.* at 1123. Under the court's new rule, "[o]pen driveways, unenclosed porches, basement doors left unlocked, back doors left ajar, yard gates left unlatched, garage doors that don't quite close . . . will all be considered invitations for police to sneak in." *Id.* Chief Judge Kozinski framed the decision as a product of the lack of socio-economic diversity on the bench:

> No truly poor people are appointed as federal judges, or as state judges for that matter. Judges, regardless of race, ethnicity or sex, are selected from the class of people who don't live in trailers or urban ghettos. . . . Yet poor people are entitled to privacy, even if they can't afford all the gadgets of the wealthy for ensuring it. Whatever else one may say about Pineda-Moreno, it's perfectly clear that he did not expect—and certainly did not consent—to have strangers prowl his property in the middle of the night and attach electronic tracking devices to the underside of his car. No one does. When you glide your BMW into your underground garage or behind an electric gate, you don't need to worry that somebody might attach a tracking device to it while you sleep. But the Constitution doesn't prefer the rich over the poor; the man who parks his car next to his trailer is entitled to the same privacy and peace of mind as the man whose urban fortress is guarded by the Bel Air Patrol.

Id.

173. *See* Adam Cohen, *The Government Can Use GPS to Track Your Moves*, TIME, Aug. 25, 2010, http://www.time.com/time/nation/article/0,8599,2013150,00.html.

174. No. 10-10067, 2010 WL 4595522 (D. Mass. Nov. 10, 2010). Other district court cases holding that GPS surveillance does not require a warrant include *United States v. Jesus-Nunez*, No. 10-CR-00017-01, 2010 U.S. Dist. LEXIS 76107 (M.D. Pa. Jul. 27, 2010), *United States v. Burton*, 698 F. Supp. 2d 1303 (N.D. Fla. 2010), *Morton v. Nassau Cnty. Police Dep't*, No. 05-CV-4000, 2007 WL 4264569 (E.D.N.Y. Nov. 27, 2007), and *United States v. Moran*, 349 F. Supp. 2d 425 (N.D.N.Y. 2005).

175. *Sparks*, 2010 WL 4595522, at *2.

hicle, witnessed the defendant using the car as a getaway vehicle in what turned out to be another bank robbery.[176] The defendant challenged both the installation and monitoring of the GPS device, claiming that he had a reasonable expectation of privacy in his vehicle while it was parked in a private parking lot.[177] Furthermore, the defendant argued, he maintained a reasonable expectation of privacy in the aggregate of his movements twenty-four hours per day because of the pervasive intrusion enabled by GPS technology and the improbability of the police conducting twenty-four hour surveillance visually.[178]

In regards to the installation of the GPS device, the court held that the defendant had no reasonable expectation of privacy in the residential parking lot, both because it was not part of his curtilage and because it constituted a "common area" of the apartment building open to all residents.[179] The defendant also exhibited no expectation of privacy in the exterior of his vehicle because he made no efforts "to protect or shield his vehicle from passersby," such as utilizing "an enclosed parking garage, cover[ing] his vehicle, or otherwise remov[ing] it from public view."[180] Noting that motor vehicles in general are entitled to a significantly diminished expectation of privacy,[181] the court held that the exterior or undercarriage of a vehicle is even further diminished "because it is thrust into the public eye, and thus to examine it does not constitute a search."[182] The court found that the defendant similarly did not have a reasonable expectation in his movements twenty-four hours a day because warrantless visual surveillance would have revealed to the FBI all of the information provided by the GPS device.[183] New technologies, the court reasoned, did not necessarily warrant reevaluation of Supreme Court precedent; indeed, "highly sophisticated tools" like radios, street cameras, radar, helicopters, computers, and

176. *Id.*

177. *Id.* at *5.

178. *Id.* at *7. The defendant's arguments are based largely upon the D.C. Circuit's rationale in *United States v. Maynard*, 615 F.3d 544 (D.C. Cir. 2010), holding GPS surveillance constitutes a search. *See infra* notes 235-252 and accompanying text.

179. *Sparks*, 2010 WL 4595522, at *4-5. In a "modern urban multifamily apartment house," the court reasoned, the tenant's "dwelling" does not extend beyond his individual apartment, and thus the area of the curtilage is necessarily more limited. *Id.* at *4.

180. *Id.* at *5. While such a rule was "admittedly asking a lot" of defendants, the court reasoned that the defendant was asking for just as much by asking the court to "protect that which he did not." *Id.*

181. *Id.* (citing Cardwell v. Lewis, 417 U.S. 583 (1974) (holding that there was no Fourth Amendment violation where law enforcement removed paint scrapings from a parked car)).

182. *Id.* (citing New York v. Class, 475 U.S. 106, 114 (1986)).

183. *Id.* at *9. Furthermore, the Fourth Amendment does not prohibit police from augmenting their sensory abilities, nor has the Supreme Court has ever "equated police efficiency with unconstitutionality." *Id.*

license and fingerprint databases produce more accurate fact-finding and further the cause of justice.[184] If a technology merely provided "a replacement for an activity that is not a search . . . use of that technology does not render the activity illegal."[185]

In response to the defendant's argument that prolonged surveillance and the aggregation of his travels produced a more intrusive glimpse into his life than would be available via traditional visual surveillance,[186] the court found that while "continuous monitoring may capture quantitatively more information than brief stints of surveillance," the type of information collected was "qualitatively the same."[187] Meanwhile, creating a rule based on the length of the surveillance would produce unclear guidelines for law enforcement and could even outlaw visual surveillance.[188] Furthermore, the court dismissed the defendant's probabilistic argument by citing to the Supreme Court's statement in *Jacobsen*[189] that "the mere expectation . . . that certain facts will not come to the attention of the authorities" does not lend an individual a reasonable expectation of privacy.[190] As evidence, the court noted that while citizens might not expect government agents to rifle through their trash on the curb or rent an airplane to conduct aerial surveillance of their residence, those actions are not unreasonable searches in Fourth Amendment jurisprudence.[191]

Finally, the court found the defendant had no reasonable expectation of privacy because citizens are generally aware of the use and "power" of GPS technology.[192] As examples of this awareness, the court cited to the proliferation of private use of GPS, media reports of law enforcement's use of GPS technology to track Scott Peterson in the aftermath of his wife's

184. *Id.*

185. *Id.* at *8 (citing Kyllo v. United States, 533 U.S. 27, 34 (2001)).

186. The defendant was positing a theory expressed in several recent cases, including *United States v. Maynard*, 615 F.3d 544 (D.C. Cir. 2010), that the whole of a person's movements over time reveals more than the sum of its parts and deserves Fourth Amendment protection. *See also* April A. Ottenberg, 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, 685 n.171, 697-98 (2005) (suggesting that the aggregation of one's movements constitutes a "private space" under the Fourth Amendment and that courts should require a warrant for prolonged surveillance).

187. *Sparks*, 2010 WL 4595522, at *8.

188. *Id.*

189. United States v. Jacobsen, 466 U.S. 109, 122 (1984).

190. *Sparks*, 2010 WL 4595522, at *7 (citing *Jacobsen*, 466 U.S. at 122). For a discussion of probabilistic reasoning, see *supra* note 117 and accompanying text.

191. *Sparks*, 2010 WL 4595522, at *7 (citing California v. Greenwood, 486 U.S. 35 (1988), and California v. Ciraolo, 476 U.S. 207 (1986)).

192. *Id.*

death,[193] news articles about the "widespread government surveillance" conducted by the Bush administration,[194] and the government's reported attempts to require communications service providers like BlackBerry and Facebook "to be technologically capable of complying with a wiretap order if served."[195] Thus, the court reasoned, even if the defendant had maintained a subjective expectation of privacy, because of the reported widespread use of the technology, society would not recognize that expectation as reasonable.[196] Even in declaring that GPS surveillance did not require a warrant, the court stressed that its holding should not be interpreted to allow the government "to stride, unchecked, through this technological age."[197] However, in the tradeoff between security and privacy, the ability of the government to protect the public through the use of bourgeoning technology triumphed.[198]

2. State Courts Finding No Search or Seizure

While several states have addressed the issue of GPS tracking, many do so under the guise of their State Constitution.[199] One recent case to hold that GPS surveillance does not constitute a search under both the Virginia State Constitution and the Fourth Amendment is *Foltz v. Commonwealth*.[200] In that case, the Fairfax County police used a GPS device to

193. *Id.* (citing *Judge Allows GPS Evidence in Peterson Case*, CNN.COM (Feb. 17, 2004), http://www.cnn.com/2004/LAW/02/17/peterson.trial/index.html).

194. *Id.* at *10 n.16 (citing James Risen & Eric Lichtblau, *Bush Lets U.S. Spy on Callers Without Courts*, N.Y. TIMES, Dec. 16, 2005, at A1, *available at* http://www.nytimes.com/2005/12/16/politics/16program.html).

195. *Id.* (citing Charlie Savage, *U.S. Tries to Make it Easier to Wiretap the Internet*, N.Y. TIMES, Sept. 27, 2010, at A1, *available at* http://www.nytimes.com/2010/09/27/us/27wiretap.html).

196. *Id.* at *7.

197. *Id.* at *10.

198. *Id.*

199. *See* People v. Weaver, 909 N.E.2d 1195, 1202 (N.Y. 2009); State v. Campbell, 759 P.2d 1040, 1041 (Or. 1988); State v. Jackson, 76 P.3d 217, 220 (Wash. 2003).

200. 698 S.E.2d 281 (Va. Ct. App. 2010). The Nevada Supreme Court held similarly in *Osburn v. State*, 44 P.3d 523, 526 (Nev. 2002), that attachment of an electronic beeper did not constitute a search or seizure within the meaning of either the Nevada Constitution or the Fourth Amendment. The court followed the Ninth Circuit's reasoning in *McIver* that there was no indication the defendant had a subjective expectation of privacy in the exterior of his vehicle because he did not take any steps to shield or hide the area from inspection by others and the vehicle was parked in plain view on the street. *Id.* The dissent in *Osburn* took issue with this analysis, noting that "[i]f we focus only on a person's expectation of privacy for his bumper . . . I believe we are missing the real impact of the intrusion on a person's privacy," for "placing a monitor on an individual's vehicle effectively tracks that person's every movement just as if the person had it on his or her person." *Id.* at 527 (Rose, J., dissenting).

track a registered sex offender in his company van when they suspected him of being involved in a new string of sexual assaults in Northern Virginia.[201] From observing the defendant's daily movements, they were able to determine that the recent assaults occurred in areas near where the defendant worked and attended meetings.[202] Using the GPS device and visual surveillance, the police were able to apprehend the defendant as he attempted to commit another sexual assault.[203] After finding that the privacy rights in the Virginia Constitution are coextensive with those in the United States Constitution, the court followed most federal courts to hold that that GPS surveillance did not constitute a search because the defendant had no reasonable expectation of privacy in his movement on public roads and showed no subjective expectation of privacy in the bumper of the vehicle.[204] The court reasoned that the defendant did nothing to prevent others from inspecting the bumper of the work van, for "the vehicle was not parked on private property" and "the police did not need to remove a lock, latch, or cover to reach into the bumper and attach the GPS device."[205] Furthermore, the installation of the device did not constitute a seizure because the defendant did not own the van, and thus it did not meaningfully interfere with the defendant's possessory interests.[206] The court did distinguish the tracking conducted by police in *Foltz* (which lasted "at most six days") from other cases in which police tracked suspects for weeks or months at a time, suggesting that greater privacy interests might be at stake in the latter cases.[207]

B. Cases Holding GPS Surveillance Requires a Warrant

While the "split" over GPS surveillance was formerly more lopsided in favor of not requiring a warrant, in 2010 the "pro-warrant" side gained significant momentum with the first federal circuit court ruling expressly that both the installation and tracking of a GPS device on a vehicle constituted a search.[208] Before the D.C. Circuit's ruling however, several lower and state courts reached this conclusion first.

201. *Foltz*, 698 S.E.2d at 283.

202. *Id.*

203. *Id.* at 284.

204. *Id.* at 286.

205. *Id.* at 286-87.

206. *Id.* at 287-88. The court did not decide the question of whether the installation would have constituted a seizure if the defendant had owned the van. *Id.* at 288 n.10.

207. *Id.* at 291 n.12 (referring to *United States v. Maynard*, 615 F.3d 544 (D.C. Cir. 2010), where police tracked the defendant's vehicle for four weeks).

208. *See infra* Part II.B.2.

1. State Courts Lead Off the Pro-Warrant Analysis

As discussed in Part I, prior to the Supreme Court's decision in *United States v. Knotts*, the Fifth Circuit in 1976 refused to hold that every citizen "runs the risk that the government will plant a bug in his car in order to track his movements, merely because he drives his car in areas accessible to the public."[209] However in the wake of *Knotts*, it was the state courts that first held that the use of beepers, and then GPS surveillance, constituted a search and seizure.[210] For example, in 2003 the Oregon Supreme Court held in *State v. Campbell* that overt attachment and use of beeper was a search and seizure under the Oregon Constitution, violating the defendant's constitutional rights in the absence of a warrant or exigent circumstances.[211] First, the court argued, the idea that an electronic tracking device merely replaced visual surveillance was "factually unsound," for a beeper "broadcasts a signal that enables the police to locate, with little delay, the transmitter from anywhere that its signal can be received."[212] As proof, the court pointed out that "the police, notwithstanding diligent efforts, found it impossible to follow the defendant's automobile through visual surveillance."[213] Furthermore, the court found the differentiation as to where the defendant traveled in his car—on public roads, or on private property—to be a useless distinction, for "whether using the transmitter is a search cannot depend upon the fortuity of where the transmitter happens to be taken by the person under observation. In order to decide whether the government has search, we must look to the nature of the act."[214] As to the nature of that act, the court was certain: "any device that enables police quickly to locate a person or object within a 40-mile radius, day or night," and offers no means for an individual to "ascertain when they were being scrutinized" was "nothing short of a staggering limitation upon personal freedom."[215]

In 2009, two more state cases came down on the side of search and seizure, specifically in the context of GPS surveillance. The first was *People v. Weaver*,[216] a landmark decision by the New York State Court of Ap-

209. United States v. Holmes, 521 F.2d 859, 865 (5th Cir. 1975), *aff'd en banc*, 537 F.2d 227; *see also supra* notes 95-98 and accompanying text.

210. *See, e.g.*, Commonwealth v. Connolly, 913 N.E.2d 356, 361 (Mass. 2009); People v. Weaver, 909 N.E.2d 1195, 1202 (N.Y. 2009); State v. Campbell, 759 P.2d 1040, 1041 (Or. 1988); State v. Jackson, 76 P.3d 217, 220 (Wash. 2003).

211. 759 P.2d at 1041.

212. *Id.* at 1045.

213. *Id.*

214. *Id.* at 1047.

215. *Id.* at 1048-49.

216. 909 N.E.2d 1195 (N.Y. 2009).

peals, which held in a 4-3 ruling that the placement and monitoring of a GPS tracking device constituted a search under the New York Constitution,[217] utilizing what would become known as the "mosaic theory" of GPS surveillance.[218] In *Weaver*, police installed a GPS device inside the bumper of defendant's car and monitored it for sixty-five days.[219] The court distinguished the case from *Knotts* by finding first that GPS was a "vastly different and exponentially more sophisticated and powerful" technology than a beeper.[220] Rather than simply augmenting human senses like a searchlight or binoculars, GPS technology "facilitate[d] 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 of time."[221] Unlike the primitive beepers of *Knotts*, with GPS technology, no human tracking was necessary and surveillance was essentially uninterrupted.[222] Furthermore, the court refused to analogize GPS to visual surveillance, because the visual "equivalent" to GPS technology would require millions of police officers on every corner of every street—a budgetary and logistical impossibility.[223]

Furthermore, the court held, GPS technology allowed police to view "the whole of a person's progress through the world, into both public and private spatial spheres."[224] With the instantaneous transmission of GPS information, police could access an aggregation of location data, "the indisputably private nature of which takes little imagination to conjure," including "trips to the psychiatrist, the plastic surgeon, the abortion clinic, the AIDS treatment center, the strip club, the criminal defense attorney, the by-the-hour motel, the union meeting, the mosque, synagogue or church [and] the gay bar."[225] The resulting picture, the court reasoned, was a "highly detailed profile, not simply of where we go, but by easy inference, of our associations—political, religious, amicable and amorous, to name only a few—and of the pattern of our professional and vocational pur-

217. *Id.* at 1202. While it contains additional language concerning telephonic communications, the Fourth Amendment analogue in the New York Constitution is nearly identical to that in the federal Constitution. N.Y. CONST. ART. I, § 12.

218. The "mosaic theory" posits that the whole of a person's movements over time reveals more than the sum of its parts. *See* United States v. Maynard, 615 F.3d 544, 562 (D.C. Cir. 2010); *see also* Ottenberg, *supra* note 186.

219. *Weaver*, 909 N.E.2d at 1195.

220. *Id.* at 1199.

221. *Id.*

222. *Id.*

223. *Id.*

224. *Id.*

225. *Id.*

suits."[226] An individual's expectation of privacy, the *Weaver* court held, was not so utterly diminished that he would effectively consent to this kind of invasion.[227]

Finally, the court stressed the procedural nature of the Fourth Amendment and noted that multiple exceptions to the warrant requirement could still apply, for there "likely will be exigent situations in which the requirement of a warrant issued upon probable cause authorizing the use of GPS devices for the purpose of official criminal investigation will be excused."[228]

The Supreme Court of Massachusetts ruled in accordance with New York's highest court shortly after, holding that the installation of a GPS device to a minivan required a warrant because it constituted both a search and seizure.[229] One of the few courts to rule explicitly on the issue of seizure, the court in *Connolly* held that the seizure requirement was met because installation of a GPS device constituted a meaningful interference with the defendant's possessory rights.[230] Relying on Justice Stevens' analysis in *United States v. Karo*, the court found the government had interfered with two of the defendant's possessory interests. By using the GPS device to continually track his movement without his knowledge, law enforcement had substantially infringed on the defendant's right "to exclude others from his vehicle," as well as his right to the "use and enjoyment of his vehicle."[231] In contrast to the Seventh Circuit in *Garcia*, the court held that a seizure could occur regardless of whether the device drew power from the vehicle.[232] Rather, a seizure occurs "not by virtue of the technology employed, but because the police use private property (the vehicle) to obtain information for their own purposes."[233] As to the monitoring of the device, the court found that the defendant could maintain a reasonable expectation of privacy in his location twenty-four hours a day because "[d]espite the increasing use of sophisticated technological devices, there has not been a corresponding societal expectation that government authorities will use such devices to track private citizens."[234]

226. *Id.* at 1199-1200.

227. *Id.* at 1200.

228. *Id.* at 1201.

229. Commonwealth v. Connolly, 913 N.E.2d 356, 361 (Mass. 2009).

230. *Id.* at 370.

231. *Id.* (citing United States v. Karo, 468 U.S. 705, 729 (1984) (Stevens, J., dissenting)).

232. *Id.* at 370. For a discussion of the Seventh Circuit's decision in *Garcia*, see *supra* notes 143-149 and accompanying text.

233. *Connolly*, 913 N.E.2d at 370.

234. *Id.* at 369.

2. The Bourgeoning Split: The District of Columbia Court of Appeals Weighs In

In 2010, the Court of Appeals for the District of Columbia became the first federal circuit court to hold that warrantless use of a GPS device on a defendant's vehicle for a month constituted a search that required a warrant.[235] With facts that could have been drawn directly from the television series *The Wire*,[236] in *United States v. Maynard*, law enforcement officers investigating two owners of a D.C. night club for narcotics violations, installed and monitored a GPS device on one of the defendant's vehicles for four weeks without a valid warrant.[237] The court found that *Knotts*[238] was not controlling and held that GPS surveillance of the defendant's car twenty-four hours per day defeated the defendant's reasonable expectation of privacy.[239] In fact, the D.C. Circuit noted, the Supreme Court in *Knotts* specifically reserved the question of whether a warrant would be required in cases involving "twenty-four hour surveillance."[240] Furthermore, in holding that an individual traveling by car on public roads had no reasonable expectation of privacy in his movements from one place to another, the Court in *Knotts* emphasized the "limited information discovered by use of

235. United States v. Maynard, 615 F.3d 544, 563 (D.C. Cir. 2010), *reh'g en banc denied sub nom.* United States v. Jones, 625 F.3d 766, *cert. denied*, Maynard v. United States, No. 10-7102, 2010 WL 4156203 (Nov. 29, 2010).

236. *The Wire* is an American television drama that examined the intersection of law enforcement, illegal drug trade, print news media, and the political, educational, and governmental systems of Baltimore, Maryland. *See The Wire* (HBO television series June 2, 2002-Mar. 9, 2008); *see also* Orin Kerr, *D.C. Circuit Introduces "Mosaic Theory" of Fourth Amendment, Holds GPS Monitoring a Fourth Amendment Search*, THE VOLOKH CONSPIRACY (Aug. 6, 2010, 2:46 PM), http://volokh.com/2010/08/06/d-c-circuit-introduces-mosaic-theory-of-fourth-amendment-holds-gps-monitoring-a-fourth-amendment-search/ (similarly noting the parallels between the facts of *Maynard* and *The Wire*).

237. *Maynard*, 615 F.3d at 555.

238. 460 U.S. 276 (1983).

239. *Maynard*, 615 F.3d at 555-56. In so holding, the court noted that the defendants in two of the three federal circuits to already decide the issue—*Garcia* and *Marquez*—explicitly conceded that the monitoring of the GPS device was not a search, instead contesting only the installation. *Id.* at 557-58 (citing Brief of Appellant at 22, United States v. Garcia, 474 F.3d 994 (7th Cir. 2007) (No. 06-2741) ("Garcia does not contend that he has a reasonable expectation of privacy in the movements of his vehicle while equipped with the GPS tracking device as it made its way through public thoroughfares. . . . His challenge rests solely with whether the warrantless installation of the GPS device, in and of itself, violates the Fourth Amendment.")). Furthermore, all three cases expressly reserved the issue of whether "wholesale surveillance" would require a warrant. *Id.* at 558.

240. *Id.* at 556 (citing United States v. Knotts, 460 U.S. 276, 283-84 (1983)). For a discussion of how GPS, unlike beeper technology, enables twenty-four surveillance, see *supra* notes 15, 17-19 and accompanying text.

the beeper."[241] Such a holding, the D.C. Circuit found, did not indicate that a person has "no reasonable expectation of privacy in his movements whatsoever, world without end, as the Government would have it."[242]

From this basis, the court considered anew whether a GPS device, which enables twenty-four hour surveillance over extended periods of time, violated the reasonable expectation of privacy test set forth in *Katz*.[243] Under the first prong of the *Katz* test, whether an expectation of privacy is reasonable "depends in large part upon whether that expectation relates to information that has been 'expose[d] to the public.'"[244] An individual "does not leave his privacy behind when he walks out his front door"; rather, "what [one] seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected."[245] The D.C. Circuit found that the defendant retained a reasonable expectation of privacy in his movements twenty-four hours a day because he did not actually or constructively expose his movements over the course of a month to the public:

> First, unlike one's movements during a single journey, the whole of one's movements over the course of a month is not *actually* exposed to the public because the likelihood anyone will observe all those movements is effectively nil. Second, the whole of one's movements is not exposed *constructively* even though each individual movement is exposed, because that whole reveals more—sometimes a great deal more—than does the sum of its parts.[246]

Moreover, the court distinguished between the *possibility* that an act might occur and the *expectation* that it will occur: "In considering whether something is 'exposed' to the public . . . we ask not what another person can physically and may lawfully do but rather what a reasonable person expects another might actually do."[247] Thus, whether something is "expose[d] to the public," depends not upon the theoretical possibility, but upon the actual likelihood, of discovery by a stranger.[248] The fact that a stranger could never actually see the aggregation of an individual's movements over forty days indicated the individual has not actually exposed that information to the public.[249]

241. *Id.* (citing *Knotts*, 460 U.S. at 283 (noting the "limited use which the government made of the signals from this particular beeper")).

242. *Id.* at 557.

243. *Id.* at 558.

244. *Id.* (quoting Katz v. United States, 389 U.S. 347, 351 (1967)).

245. *Id.* at 563 (quoting *Katz*, 389 U.S. at 351).

246. *Id.* at 558.

247. *Id.* at 559.

248. *Id.* at 560 (citing *Katz*, 389 U.S. at 351).

249. *Id.*

The court in *Maynard* also introduced what they coined the "mosaic theory," which posited that the whole of a person's movements over time revealed more than the sum of its parts, and deserved Fourth Amendment protection:[250]

> Repeated visits to a church, a gym, a bar, or a bookie tell a story not told by any single visit. . . . 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.[251]

Thus, prolonged surveillance revealed a certain quality of information not revealed by individual trips viewed in isolation.[252]

As to the objective prong of the *Katz* test, the court noted that even where a defendant's movements were not exposed to the public, his expectation of privacy in those movements is not necessarily reasonable. Rather, the "legitimation of expectations of privacy must have a source outside the Fourth Amendment," which provides evidence of "understandings that are recognized or permitted by society."[253] The D.C. Circuit began by looking at statutes such as California's, which declares that "electronic tracking of a person's location without that person's knowledge violates that person's reasonable expectation of privacy," thereby requiring a warrant for a GPS device.[254] While state laws may not be conclusive evidence of nationwide "societal understandings," the court found that they were "indicative that

250. *Id.* at 562; *see also supra* note 186.

251. *Id.*

252. *Id.* As support for this analysis, the D.C. Circuit referred to *U.S. Dep't. of Justice v. Reporters Comm. for Freedom of the Press*, 489 U.S. 749 (1989) as precedent. In *Reporters Comm.*, the respondents had requested from the FBI certain rap sheets pursuant to a Freedom of Information Act (FOIA) request. *Id.* at 749. The Court held that while "individual events in those summaries [were] matters of public record," the subjects had a privacy interest in the aggregated record as opposed to the "bits of information" of which it was composed. *Id.* at 764. Thus, the disclosure of the entire rap sheet "could reasonably be expected to constitute an unwarranted invasion of personal privacy." *Id.*

253. *Maynard*, 615 F.3d at 563 (quoting United States v. Jacobsen, 466 U.S. 109, 123 n.22 (1984)).

254. *Id.* at 564 (citing CAL. PENAL CODE § 637.7 (West 2010), 1998 Cal. Stat. 449, § 2); *see also* HAW. REV. STAT. §§ 803-42, 803-44.7 (2010) (requiring a "search warrant" for installation of a "mobile tracking device"); OKLA. STAT. tit. 13, §§ 176.6, 177.6 (2010) (requiring a showing of probable cause for the issuance of a warrant for installation of a tracking device); S.C. CODE ANN. § 17-30-140 (2010) (requiring a finding of "probable cause" for a mobile tracking device).

prolonged GPS monitoring defeats an expectation of privacy that our society recognizes as reasonable."[255] These statutes, in addition to the decisions of other courts to which the issue had been "squarely presented," and the general intrusiveness of GPS technology, led the court to "only one conclusion: Society recognizes [the defendant's] expectation of privacy in his movements over the course of a month as reasonable."[256] GPS surveillance, therefore, defeated both prongs of the *Katz* test and required a warrant.

C. The Intersection of GPS and Cell Phone Surveillance Case Law

1. Background: Cell-Site Technology, Statutory Authority and Case Law

As discussed in Part I, the government has an entirely separate mode of conducting twenty-four hour surveillance through cell phones.[257] The legal discussion surrounding cell phone data is somewhat distinguishable from the tracking of vehicles because communications information is governed by several federal communications statutes as well as the Third Party Doctrine.[258] However, several recent cases to analyze the legal standard for cell-site information (CSI)[259] have closely paralleled the discussions of an individual's reasonable expectation of privacy present in cases addressing attachment of a GPS device to a vehicle.[260] The primary difference in CSI cases is that the "tracking device" is the individual's cell phone.

The first issue in cell phone surveillance analysis is whether any of the several federal statutes governing electronic communications allow the disclosure of particular CSI and which standard of cause applies. The Electronic Communications Privacy Act (ECPA),[261] enacted in 1986 in an attempt to strike "a fair balance between the privacy expectations of American citizens and the legitimate needs of law enforcement agencies,"[262] authorized various criminal investigative tools under four different

255. *Maynard*, 615 F.3d at 564.

256. *Id.* at 563.

257. *See generally ECPA Hearing*, *supra* note 20 (statement of Prof. Matthew A. Blaze).

258. *See supra* note 121.

259. For purposes of this discussion, cell-site information (CSI) refers to non-GPS cell tower triangulation location data, which is currently the most pervasive method of cell phone tracking. *See ECPA Hearing*, *supra* note 20, at 22 (statement of Prof. Matthew A. Blaze). Furthermore, no published opinions have allowed access to cell phone GPS data on a showing of less than probable cause. *See id.* at 84 (statement of Stephen Wm. Smith, U.S. Mag. J.).

260. *See infra* Part II.C.2.

261. Pub. L. No. 99-508, 100 Stat. 1848 (1986) (codified as amended in scattered sections of 18 U.S.C.).

262. Recent Development, *supra* note 14, at 312.

legal standards. First, pen registers and trap/trace devices have the least demanding standard (the information sought must be "relevant to an ongoing investigation."[263] Second, stored communications and account records are accessible with "specific and articulable facts."[264] Third, tracking device warrants are covered by Rule 41's "probable cause" standard.[265] Fourth, wiretap orders have a "super-warrant" requirement.[266]

The challenge for courts in ruling on CSI disclosure is that the ECPA does not define the standard for either cellular tower location data or GPS information from a cell phone.[267] The Stored Communications Act (SCA),[268] which prohibits electronic communications providers from disclosing stored customer information unless under appropriate legal authority, also lists cell phone records[269] under the legal standard of "specific and articulable facts."[270] However, the SCA explicitly *excludes* from the definition of electronic communications "any communication from a tracking device," which is defined as "an electronic or mechanical device which permits the tracking of the movement of a person or object."[271] Furthermore, when Congress passed the Communications Assistance for Law Enforcement Act (CALEA),[272] which required telecommunications carriers to aid in intercepting digital communications, it specifically noted that any information acquired solely pursuant to a pen register or trap and trace device "shall not include any information that may disclose the physical location of the subscriber."[273] Thus the primary issue for magistrate judges comes down to whether location information from a cell phone—either from cellular tower triangulation or GPS data—should be interpreted as a "commu-

263. *ECPA Hearing*, *supra* note 20, at 82 (statement of Stephen Wm. Smith, U.S. Mag. J.); *see also* 18 U.S.C. § 3122 (2006).

264. *ECPA Hearing*, *supra* note 20, at 82 (statement of Stephen Wm. Smith, U.S. Mag. J.) (citing 18 U.S.C. § 2703 (2006)).

265. *Id.* (citing 18 U.S.C. § 3117 (2006)); *see also* FED. R. CRIM. P. 41.

266. *ECPA Hearing*, *supra* note 20, at 82 (statement of Stephen Wm. Smith, U.S. Mag. J.).

267. *See id.* at 81-83.

268. 18 U.S.C. §§ 2701-2712 (2006).

269. A "cell phone record" is defined as "a record or other information pertaining to a subscriber to or customer of such service (not including the contents of communications)." § 2703(c).

270. *See* § 2703(d).

271. *See* § 3117(b); *ECPA Hearing*, *supra* note 20, at 82 n.11 (statement of Stephen Wm. Smith, U.S. Mag. J.).

272. Pub. L. No. 103-414, 108 Stat. 4279 (1994) (codified at 47 U.S.C. §§ 1001-10 (2006)).

273. 47 U.S.C. § 1002 (a)(2)(B) (2006).

nications record" under the SCA, or information from a "tracking device."[274]

2. Cases Holding Both Prospective and Historical Cell-Site Information Require a Warrant

Interestingly enough, magistrate judges are largely in agreement that prospective, or "real-time" tracking information from a cell-phone requires a warrant substantiated by probable cause.[275] This is because the SCA applies only to "stored," or "historical" communication data.[276] In fact, "not one reported decision has ever allowed access to unlimited (i.e., multi-tower, triangulation or GPS) location data on anything other than a probable cause showing."[277] To get around this issue, however, law enforcement need only to request the information after the time period for which they want to track the suspect for it to qualify as "historical" rather than "prospective" information.[278] In turn, several magistrate judges in the past few years have ruled that *historical* CSI also requires a showing of probable cause, because it is essentially location-tracking information.[279]

274. *See ECPA Hearing*, *supra* note 20, at 82-83 (statement of Stephen Wm. Smith, U.S. Mag. J.).

275. *See id.* at 84 ("Surveying the published opinions, it is fair to conclude that the majority held that probable cause is the appropriate standard for government access to prospective cell site information."); *see also In re* Order Directing a Provider of Elec. Commc'n Serv. to Disclose Records to the Gov't, 534 F. Supp. 2d 585, 609 (W.D. Pa. 2008) [hereinafter *Lenihan Opinion*] ("[A] significant majority of Courts have rejected the Government's contention that real-time, or prospective, movement/location information may be obtained under a hybrid theory which purports to combine the authorities of the [Pen Register Statute] and the SCA by seizing upon the term 'solely' in a provision of the CALEA."), *aff'd*, No. 07-524M, 2008 WL 4191511, at *1 (W.D. Pa. Sept. 10, 2008), *vacated and remanded*, 620 F.3d 304, 319 (3rd Cir. Sept. 7, 2010).

276. *See ECPA Hearing*, *supra* note 20, at 82-83 (statement of Stephen Wm. Smith, U.S. Mag. J.) (citing 18 U.S.C. § 2510(12)(C) (2006)).

277. *Id.* at 84. Those decisions which have allowed disclosure of prospective CSI restrict their holdings to "limited CSI" only, defined as information from a particular tower or particular phone call (as opposed to multi-tower triangulation information or GPS location data). *Id.* at 83 n.16, 84. One of the inherent difficulties in assessing the decisions of magistrate judges is that most do not publish their opinions when they grant applications for orders. Thus, as Magistrate Judge Stephen Smith testified before Congress, published opinions may not be representative of judicial opinion as a whole. *Id.* at 84 n.20.

278. *See id.* at 84-85.

279. *See, e.g.*, *In re* U.S. Order Authorizing the Release of Historical Cell-Site Info., No. 10-MJ-0550, 2010 U.S. Dist. LEXIS 88781, at *1, *3 (E.D.N.Y. Aug. 27, 2010) [hereinafter *Orenstein Opinion*]; *Lenihan Opinion*, *supra* note 275; *In Re* Application For Pen Register And Trap/Trace Device With Cell Site Location Authority, 396 F. Supp. 2d 747, 757 (S.D. Tex. 2005) [hereinafter *Smith Opinion*] (rejecting the government's application for CSI on a prospective basis).

In 2008, for example, a magistrate judge in the Western District of Pennsylvania published an opinion on behalf of all magistrate judges sitting in that district, holding that both prospective and historical CSI required a showing of probable cause.[280] Writing for the court, Judge Lenihan reasoned that both the text and the legislative history of the ECPA and its amendments warranted no distinction between real-time and stored CSI.[281] A cell phone that is "used to provide the government with movement or location information," the court held, is a "tracking device" within the meaning of the SCA, and historical CSI "remains information from a tracking device."[282] Furthermore, the court wrote, even if this information were within the scope of the SCA, to read the statute that way might "erode traditional Fourth Amendment protections" and render the SCA unconstitutional.[283]

Under the court's Fourth Amendment analysis, because Rule 41 of the Federal Rules of Criminal Procedure requires a showing of probable cause for tracking devices, any interpretation that would allow disclosure at a lower standard would "violate Americans' reasonable expectation of privacy . . . as to their physical movements/locations."[284] Judge Lenihan explicitly applied the *Katz* test, finding that first, most Americans "do not generally know that a record of their whereabouts is being created whenever they travel about with their cell phones, or that such record is likely maintained by their cell phone providers and is potentially subject to review by interested Government officials."[285] Second, she wrote, "most Americans would be appalled by the notion that the Government could obtain such a record without at least a neutral, judicial determination of probable cause."[286] Citing *United States v. Karo*,[287] Judge Lenihan noted further that a cell phone travels with a person onto private property, and thus a warrant should be required.[288] However, she also criticized this "public/private dichotomy," because "routine allowance of location information

280. *See Lenihan Opinion*, *supra* note 275, at 602-03.

281. *Id.* at 610 ("The relevant legislative history indicates that Congress did not intend its electronic communications legislation to be read to require . . . disclosure of an individual's location information; to the contrary in enacting the legislation it relied on express representation by law enforcement that it was not seeking to amend the background standards governing the disclosure of movement/location information. The ECPA and the CALEA were careful to exempt this information from their reach.").

282. *Id.* at 602-03.

283. *Id.* at 610.

284. *Id.* at 610-11.

285. *Id.* at 611.

286. *Id.*

287. 468 U.S. 705 (1984).

288. *Lenihan Opinion*, *supra* note 275, at 612-13.

up to the threshold of the private domain would necessitate increasingly-difficult line-drawing at the margins."[289] Instead, she relied on the "beeper" decisions of *State v. Campbell*[290] and *State v. Jackson*[291] (both of which required a warrant for the use of an electronic tracking device) to find that that the "privacy and associational interests" of CSI disclosure implicated the Fourth Amendment, and were not "diminished by a delay in disclosure."[292]

More recently, in August of 2010, Magistrate Judge Orenstein of the Eastern District of New York issued a similar opinion holding that both prospective and historical cell-site information required a warrant under the Fourth Amendment.[293] Judge Orenstein's opinion represents the closest intersection between GPS vehicle surveillance and cell phone surveillance yet, as he relies explicitly on several GPS cases referred to in Part II.A-B of this Note.[294] The opinion also rejects the premise that increasing public awareness or use of GPS technology and location-sharing applications might diminish an individual's reasonable expectation of privacy in his movements twenty-four hours per day.[295]

In the case, the government sought an order pursuant to the SCA directing Sprint Nextel to disclose all calls and text messages, as well as certain historical CSI, from a mobile telephone for a period of fifty-eight days.[296] The government proffered "specific and articulable facts," but specifically declined to seek a warrant.[297] At the outset, Judge Orenstein noted that the case law on the issue was unsettled, resulting in "an unpredictable legal regime in which an individual's right to privacy waxes and wanes based on

289. *Id.* at 613.

290. 759 P.2d 1040, 1041 (Or. 1988).

291. 76 P.3d 217, 231 (Wash. 2003).

292. *Lenihan Opinion*, *supra* note 275, at 613. Judge Lenihan's decision was subsequently affirmed by the District Court in *In re Order Directing a Provider of Elec. Commc'n Serv. to Disclose Records to the Gov't*, No. 07-524M, 2008 WL 4191511, at *1 (W.D. Pa. Sept. 10, 2008), but was then vacated and remanded in *In re Order Directing a Provider of Elec. Commc'n Serv. to Disclose Records to the Gov't*, 620 F.3d 304, 319 (3rd Cir. 2010); however, because the Third Circuit's decision retained for magistrate judges the discretion to require probable cause for historical cell-site information, it has been seen as a victory among privacy advocates. *See* David Kravets, *Court Rebuffs Obama on Warrantless Cell-Site Tracking*, WIRED.COM (Dec. 15, 2010), http://www.wired.com/threatlevel/2010/12/cell-site-warrants.

293. *See Orenstein Opinion*, *supra* note 279.

294. *See id.* at *11-15.

295. *See id*. at *46-50.

296. *Id.* at *1.

297. *Id.* at *1-2. After the magistrate judge expressed concern to the government that recent case law might require a showing of probable cause to satisfy Fourth Amendment concerns, the government submitted a revised application stating: "Although not required, the government submits that the facts set forth herein provide . . . probable cause." *Id.* at *3.

the fortuity of the location in which an investigation is based."[298] However, Judge Orenstein wrote, even though he believed the SCA permitted him to issue the order based on a lower standard of cause, he believed that the Fourth Amendment prevented him from ordering the disclosure of the information without a showing of probable cause.[299]

In his analysis, Judge Orenstein relied heavily on the D.C. Circuit's decision in *United States v. Maynard*,[300] "both with respect to its demonstration that *Knotts* is not dispositive on the issue of prolonged location tracking," and its examination of "the privacy interest at stake when the government uses technological means to accomplish the kind of prolonged, continuous, and detailed surveillance that would otherwise be impossible."[301] In accepting these arguments, Judge Orenstein identified "a growing recognition" that:

> [T]echnology has progressed to the point where a person who wishes to partake in the social, cultural, and political affairs of our society has no realistic choice but to expose to others, if not to the public as a whole, a broad range of conduct and communications that would previously have been deemed unquestionably private.[302]

In light of these constraints on privacy, Judge Orenstein concluded that magistrate judges presented with requests for warrantless location-tracking "must carefully re-examine the constitutionality of such investigative techniques . . . it is no longer enough to dismiss the need for such analysis by relying on cases such as *Knotts*."[303]

In regards to the applicability of the Third Party Doctrine, Judge Orenstein referred to a Sixth Circuit decision, *United States v. Warshak*,[304] which found that a defendant had a reasonable expectation of privacy in the content of his emails despite his understanding that his Internet Service Provider (ISP) maintained independent access to those messages.[305] He also pointed to the Sixth Circuit's decision in *United States v. Forest*,[306] which,

298. *Id.* at *8.

299. *Id.* at *6-9.

300. 615 F.3d 544, 563 (D.C. Cir. 2010) (holding that an individual had a reasonable expectation of privacy in his movements twenty-four hours per day over a prolonged period of time, and thus attachment and monitoring of a GPS device on a vehicle required a warrant).

301. *See Orenstein Opinion*, *supra* note 279, at *19.

302. *Id.* at *11-12.

303. *Id.* at *13.

304. 490 F.3d 455 (6th Cir. 2007), *vacated and remanded*, 532 F.3d 521 (2008), *aff'd on appeal after remand*, United States v. Warshak, Nos. 08-3997, 08-4212, 08-4085, 08-4429, 08-4087, 09-3176, 2010 WL 5071766 (6th Cir. Dec. 14, 2010).

305. *Orenstein Opinion*, *supra* note 279, at *26 (citing *Warshak*, 490 F.3d at 460).

306. 355 F.3d 942 (6th Cir. 2004), *vacated sub nom.* Garner v. United States, 543 U.S. 1100 (2005).

while later vacated on other grounds, found that unlike the dialed telephone numbers, cell phone location information is not "voluntarily conveyed" by the user to cellular service providers.[307] Both cases, Judge Orenstein reasoned, demonstrated that simply because a company *could* access the content of emails or cell phone communications, "the privacy expectation in the content of either is not diminished, because there is a societal expectation that the ISP or the phone company will not do so as a matter of course."[308]

Thus, in his analysis, Judge Orenstein identified a growing tension between the Third Party Doctrine and Fourth Amendment protections when it comes to developing technology. That is, as public use of certain technology increases, and disclosure of location information to third party service providers increases, what is the attendant effect on subjective and objective reasonable expectations of privacy? As evidence of this tension, Judge Orenstein noted several growing sectors of technology where users are utilizing GPS technology through their phones, vehicles, or computers. Many cell phones now have GPS technology on them for mapping and other location-based applications.[309] Mobile phone applications such as "foursquare" allow users to "check in" at a given location, such as a bar or restaurant,

307. *See Orenstein Opinion*, *supra* note 279, at *30 (citing *Smith Opinion*, *supra* note 279, at 756-57). While the Sixth Circuit rejected the analogy between the telephone numbers in *Smith v. Maryland*, 442 U.S. 735 (1979), and cell-site information from a mobile phone, it ultimately dismissed the defendant's constitutional claims on the grounds that government surveillance took place on public highways where the defendant had no reasonable expectation of privacy. *See Orenstein Opinion*, *supra* note 279, at *30 (citing *Smith Opinion*, *supra* note 279, at 756-57).

308. *Orenstein Opinion*, *supra* note 279, at *28. In response to the government's reliance on *United States v. Miller*, 425 U.S. 435, 440 (1976), which held that an individual had no reasonable expectation of privacy in bank records on the grounds that such documents were not "private papers" but "business records of the banks," Judge Orenstein noted that the government could rely on the Bank Secrecy Act as an expression by Congress that "people should not expect to maintain privacy in financial records conveyed to banks because of the burden such privacy rights would impose on other important societal interests." *Orenstein Opinion*, *supra* note 279, at *33. In the case of cell phone location information however, the Telecommunications Act does "precisely the opposite: it expresses legislative approval for the idea that a caller should expect her location information to remain private notwithstanding the unavoidable need to share it with a third-party service provider." *Id.* (citing the Wireless Communication and Public Safety Act of 1999, Pub. L. No. 106-81, § 5, 113 Stat. 1288 (codified at 47 U.S.C. § 222(f) (2006)) ("[W]ithout the express prior authorization of the customer, a customer shall not be considered to have approved the use or disclosure of or access to . . . call location information concerning the user of a commercial mobile service.").

309. *Orenstein Opinion*, *supra* note 279, at *50. Furthermore, "[t]he Federal Communications Commission's Enhanced 911 Emergency Call Systems rules require a cellular service provider to equip mobile telephones with the ability to identify their locations to some degree of precision." *Id.* at *50-51 n.20.

and share their location with friends and other users of the service.[310] Other applications like "Google Latitude" similarly allow users to share their location with friends.[311] At the same time, Judge Orenstein noted, these applications each have privacy statements that inform the users how they can control sharing and deleting their location information.[312] Foursquare, for example, acknowledges that "an important concern for most anyone using location-based services is privacy."[313] Its privacy statement strives to make its subscribers "comfortable with how [location-tracking] information is shared via foursquare,'" and offers a range of "robust privacy controls [that] give users control over the amount of information they share about their location."[314] Google Latitude permits users to "share, set, hide your location, or sign out of Google Latitude" and to "[c]ontrol who sees your location, and at what level of detail."[315] Google Mobile, meanwhile, alerts users: "If you use location-enabled products and services, such as Google Maps for mobile, you may be sending us location information."[316]

Thus, Judge Orenstein concluded, it is very likely that "most people are—or will soon be—aware" that they are sharing location information in some capacity.[317] However, by focusing on and seeking to quiet consumers' privacy concerns over use of their location information, these companies were fostering an "actual—and to my mind reasonable—expectation that such information will remain private to the extent a subscriber chooses to make it so."[318] As further evidence of the reasonableness of privacy expectations regarding an individual's location information, Judge Orenstein cited to several articles which "illustrate [a] growing awareness and concern" surrounding use of GPS surveillance,[319] including a *Time Magazine* article which called the Ninth Circuit's holding in *United States v. Pineda-*

310. *Id.* at *47-48 (citing FOURSQUARE, http://foursquare.com/privacy).

311. *Id.* at *48 (citing GOOGLE LATITUDE, http://www.google.com/mobile/latitude).

312. *Id.* at *48-49.

313. *Id.* at *48*; see also Privacy 101*, FOURSQUARE (Dec. 20, 2010), http://foursquare.com/privacy.

314. *Orenstein Opinion*, *supra* note 279, at *48; *see also Privacy 101*, *supra* note 313.

315. *Orenstein Opinion*, *supra* note 279, at *48 (citing GOOGLE LATITUDE, http://www.google.com/mobile/latitude).

316. *Id.* (quoting *Google Mobile Privacy Policy*, GOOGLE (Dec. 14, 2010), http://www.google.com/mobile/privacy.html).

317. *Id.* at *46.

318. *Id.* at *49 n.19.

319. *Id.* at *51 n.21 (citing Cohen, *supra* note 173; Farhad Manjoo, *Facebook Knows Where You Are*, SLATE MAG. (Aug. 19, 2010), http://www.slate.com/id/2264492.

Moreno a "bizarre," "scary," and "dangerous" decision that "could turn America into the sort of totalitarian state imagined by George Orwell."[320]

Ultimately, even if mobile telephone users were aware of the fact that they expose themselves to location tracking, Judge Orenstein reasoned, that assumption did not preclude the idea that individuals still maintained a reasonable expectation of privacy in their movements: "To the contrary, I believe that a growing awareness of the *possibility* of location tracking of mobile telephones has also produced a growing expectation that such tracking can and should be controlled."[321]

Judge Orenstein's opinion represents a convergence of reasoning surrounding the issue of cell phone and vehicle surveillance by the government. This intersection makes sense for several reasons, not least of all because many citizens might not know or care about the distinctions legal scholars and judges make between such surveillance under the Third Party Doctrine or the automobile exception to the warrant. Part III of this Note further examines the intersection of these cases and argues for Judge Orenstein's and the D.C. Circuit's interpretation of an individual's reasonable expectation of privacy in his movements against twenty-four hour technological government surveillance, even in a world of increasing public use and awareness of location-based technology.

III. REVIVING PRIVACY: WHY GPS SURVEILLANCE VIOLATES THE FOURTH AMENDMENT AND SHOULD REQUIRE A WARRANT

Justice Harlan's restatement of his interpretation of the *Katz* test asked "whether under our system of government, as reflected in the Constitution, we should impose on our citizens the risks of the electronic listener or observer without at least the protection of a warrant requirement."[322] While 2010 has seen a number of privacy infractions, it has also seen a string of decisions boosting Americans' privacy interests in the age of digital technology.[323] The D.C. Circuit's decision in *Maynard*[324] and Judge Orens-

320. *See* Cohen, *supra* note 173; *see also* GEORGE ORWELL, 1984 (1949). Both GPS surveillance and cell phone surveillance often evoke references to 1984, George Orwell's novel depicting a fictional society in which government surveillance and mind control is constant and pervasive. *See* United States v. Pineda-Moreno, 617 F.3d 1120, 1121 (9th Cir. 2010) (Kozinski, C.J., dissenting) ("1984 may have come a bit later than predicted, but it's here at last."); *see also infra* notes 401, 417 and accompanying text.

321. *Orenstein Opinion*, *supra* note 279, at *46.

322. United States v. White, 401 U.S. 745, 786 (1971) (Harlan, J., dissenting).

323. *See* Kravets, *supra* note 292; *infra* notes 326-327 and accompanying text.

324. United States v. Maynard, 615 F.3d 544, 555-56 (D.C. Cir. 2010), *reh'g en banc denied sub nom.* United States v. Jones, 625 F.3d 766, *cert. denied*, Maynard v. United States, No. 10-7102, 2010 WL 4156203 (Nov. 29, 2010); *see also supra* Part II.B.2.

tein's cell-site opinion[325] were followed by two significant decisions in the ever-shifting plane of privacy jurisprudence. In December 2010, the Sixth Circuit Court of Appeals held that the government must obtain a warrant to gain access to an individual's email through an Internet service provider.[326] The following day, the Third Circuit Court of Appeals denied the Department of Justice's request for a rehearing of its decision retaining for magistrate judges the discretion to require warrants for historical cell-site information.[327] These decisions may represent a trend in cases reinforcing certain privacy rights in an age where cell phone technology, GPS devices, social networking, and Google Maps threaten to obliterate them.

In Part III of this Note, I will examine how shifting ideas of privacy affect the application of the *Katz* test to GPS surveillance. As a primary matter, I will argue that in evaluating the true nature of the implications of GPS technology under the Fourth Amendment, the installation of these devices must be examined in tandem with their monitoring capabilities. Second, I will argue for the adoption of a rule that GPS surveillance constitutes both a search and seizure under the Fourth Amendment, because the expectation that government is not tracking its citizens electronically, twenty-four hours per day, is one that society still considers legitimate.[328] Third, I will posit that neither public awareness nor popular use of location technology has eliminated an individual's reasonable expectation of privacy in his movements twenty-four hours per day.[329] Finally, I will argue that in the interest of consistency and equality in the application of Fourth Amendment protections, this "split" should be resolved in favor of a warrant.[330]

A. "The Nature of the Act": Why the Installation and Monitoring Capabilities of GPS Technology Must be Viewed Together

Part of the reason for the disarray in GPS case law is due to the challenge of applying traditional Fourth Amendment law to GPS technology, which confounds the analysis applied to searches and seizures. As discussed in Part II, courts have analyzed GPS surveillance under search and

325. *Orenstein Opinion*, *supra* note 279; *see also supra* notes 293-321 and accompanying text.

326. *See* United States v. Warshak, Nos. 08-3997, 08-4212, 08-4085, 08-4429, 08-4087, 09-3176, 2010 WL 5071766, at *1 (6th Cir. Dec. 14, 2010).

327. *In re* Order Directing a Provider of Elect. Commc'n Serv. to Disclose Records to the Gov't, No. 08-4227 (3rd Cir. Dec. 15, 2010) (denying petition for rehearing), *available at* http://www.wired.com/images_blogs/threatlevel/2010/12/3rd_circ_rehearing_denied1.pdf; *see also* Kravets, *supra* note 292.

328. *See infra* Part III.A-B.

329. *See infra* Part III.C.2.

330. *See infra* Part III.D.

seizure doctrine by looking separately at the acts of installation and monitoring.[331] However, this "bifurcated analytical framework," which has its roots in earlier beeper cases,[332] has become an overly formalistic approach that only clouds the real privacy interests at stake. This framework has also led to somewhat absurd discussions of whether a defendant has an expectation of privacy in a few inches of space on the bumper of his vehicle, when the greater privacy interest is clearly in his movements twenty-four hours per day.[333]

The complicating factor in analyzing GPS technology under the formal "search" and "seizure" inquiry is two-fold. First, the device enables a type of simultaneous search and seizure; using satellite technology, it "searches" the suspect by tracking his movements, and "seizes" by instantly digitalizing the information, storing it on the device, and transmitting it to law enforcement. Second, it is the ultimate capability of the GPS device—not the actual physical presence of the small black box—that implicates the Fourth Amendment, converting a defendant's vehicle into an instrument of the government.[334] Analyzing the installation in a vacuum, separate from its monitoring capabilities, strips the device of its Fourth Amendment significance.

In *Garcia*, for example, the Seventh Circuit found that the installation of a GPS device onto a vehicle did not constitute a seizure because the device did not: (1) affect the vehicle's driving qualities; (2) draw power from the vehicle; (3) take up room in the vehicle; or (4) alter the appearance of the vehicle.[335] This analysis is unsatisfactory however, because whether the device took up space on the vehicle or affected the vehicle's performance is irrelevant to an individual's expectation of privacy in his location data, and thus misses the extent of the government's intrusion.

B. GPS Surveillance Constitutes a Seizure Under the Fourth

331. *See supra* notes 79-98, 143-146, 229-234 and accompanying text.

332. *See* United States v. Bruneau, 594 F.2d 1190, 1194 (1979) ("[W]e adopt the Ninth Circuit's 'bifurcated analytical framework' which examines the [F]ourth [A]mendment implications of the installation or attachment of the beeper separately from the [F]ourth [A]mendment implications of monitoring its signals." (citing United States v. Miroyan, 577 F.2d 489, 492 (9th Cir. 1978))).

333. *See, e.g.*, United States v. McIver, 186 F.3d 1119, 1127 (9th Cir. 1999) (finding no search because "McIver did not produce any evidence to show that he intended to shield the undercarriage of his Toyota 4Runner from inspection by others").

334. *See* Osburn v. State, 44 P.3d 523, 527 (Nev. 2002) (Rose, J., dissenting) ("If we focus only on a person's expectation of privacy for his bumper . . . I believe we are missing the real impact of the intrusion on a person's privacy [because] placing a monitor on an individual's vehicle effectively tracks that person's every movement just as if the person had it on his or her person.").

335. United States v. Garcia, 474 F.3d 994, 996 (7th Cir. 2007).

Amendment

Rather, as the Oregon Supreme Court in *Campbell* wrote, "[i]n order to decide whether the government has searched, we must look to the nature of the act."[336] The same can be said for whether an object has been "seized." In fact, though it has received substantially less analysis,[337] some have argued that the case for seizure may be even stronger than for search.[338] After all, it is in part the attachment of a technological device to private property that separates GPS surveillance from visual surveillance. While the Supreme Court did not decide the issue in *Knotts*, Justice Brennan wrote that the case would have been a much more difficult one "if respondent had challenged [the beeper's] original installation."[339]

Indeed, examining the full capabilities of a GPS device in tandem with its monitoring capabilities demonstrates that the attachment of the device itself likely constitutes a seizure under Fourth Amendment jurisprudence. While the *Garcia* court only focused on whether a GPS device created any physical interference with the vehicle's use,[340] a seizure of property occurs whenever there is some "meaningful interference with an individual's possessory interest in that property."[341] Moreover, the government's assertion of "dominion and control" over private property may be enough to constitute a seizure.[342]

Specifically, GPS can be said to constitute a seizure in two ways. First, by using the GPS device to continually track an individual's movements without his knowledge, law enforcement is infringing on his right to exclude others from his property.[343] Second, GPS surveillance interferes with an individual's use and enjoyment of his property, for if law enforcement

336. State v. Campbell, 759 P.2d 1040, 1047 (Or. 1988).

337. *See* Kothari, *supra* note 40, at 4 ("Because most seizures follow a search, the seizure prong of the Amendment has received little scholarly or judicial notice.").

338. *See, e.g.*, *McIver*, 186 F.3d at 1134 (Kleinfeld, J., concurring) ("[T]he owner of a vehicle has a possessory interest that is meaningfully interfered with if a transmitter is installed, even where the installation does not interfere with a reasonable expectation of privacy."); Kothari, *supra* note 40, at 4-5 ("[S]eizure law . . . provides a better response to the applications of GPS technology than does search doctrine.").

339. United States v. Knotts, 460 U.S. 276, 286 (1983) (Brennan, J., concurring).

340. *See Garcia*, 474 F.3d at 996.

341. United States v. Jacobsen, 466 U.S. 109, 113 (1984).

342. *Id.* at 120.

343. *See* United States v. Karo, 468 U.S. 705, 729 (1984) (Stevens, J., concurring in part and dissenting in part) ("The owner of property, of course, has a right to exclude from it all the world, including the Government, and a concomitant right to use it exclusively for his own purposes. When the Government attaches an electronic monitoring device to that property, it infringes that exclusionary right; in a fundamental sense it has converted the property to its own use."); Commonwealth v. Connolly, 913 N.E.2d 356, 369-70 (Mass. 2009).

had the legal ability to attach a tracking device to any vehicle without a warrant, simply using a vehicle would necessitate an individual's submission to constant government surveillance.[344] Both of these interferences are "meaningful" ones, as they make it virtually impossible to conceal private property from possession and location by the government.[345]

C. GPS Surveillance Constitutes a Search Under the Fourth Amendment

Furthermore, GPS surveillance constitutes a "search" under the *Katz* test. As a threshold issue, GPS surveillance is not controlled by *Knotts*[346] for several reasons. First, *Knotts* applied to an electronic beeper, which provided tracking for a limited duration of time, and the Court expressly reserved the matter of twenty-four hour surveillance for future determination.[347] Second, GPS technology provides a much more intimate view of an individual's life.[348] Finally, *Knotts* did not decide the issue of the attachment of the device itself to an individual's personal property.[349] Therefore, we must return to the Supreme Court's doctrine in *Katz* and examine subsequent case law to determine whether this type of government action violates an individual's reasonable expectation of privacy.

1. Exhibiting Subjective Expectations: The Difficulty of Katz*' First Prong*

Regardless of its murky or circular nature, the *Katz* test survives in its two-prong form. The test is arguably complicated by Justice Harlan's iteration of the first prong, which asks whether the defendant "exhibited" a subjective expectation of privacy in the information he seeks to protect.[350] Because of the logistical ease of installing and monitoring GPS tracking devices (especially after the Ninth Circuit's holding that law enforcement can attach a device to a car while it is parked in a driveway),[351] it is quite difficult to "exhibit" an expectation of privacy in the aggregation of one's

344. *See Connolly*, 913 N.E.2d at 370.

345. *See Karo*, 468 U.S. at 730 (Stevens, J., concurring in part and dissenting in part).

346. United States v. Knotts, 460 U.S. 276 (1983).

347. *See* United States v. Maynard, 615 F.3d 544, 555-56 (D.C. Cir. 2010) (quoting *Knotts*, 460 U.S. at 283-84), *reh'g en banc denied sub nom.* United States v. Jones, 625 F.3d 766, *cert. denied*, Maynard v. United States, No. 10-7102, 2010 WL 4156203 (Nov. 29, 2010).

348. *See supra* notes 224-227, 250-252 and accompanying text.

349. *See supra* notes 79-81 and accompanying text.

350. *See* Harper, *supra* note 60, at 1386.

351. United States v. Pineda-Moreno, 591 F.3d 1212, 1214-15 (9th Cir. 2010), *reh'g denied*, 617 F.3d 1120.

twenty-four hour location data.[352] As the Fifth Circuit has noted, there is no "protective cloak" that can cover a vehicle to indicate a greater expectation of privacy.[353]

It does not follow however, that people do not maintain a subjective expectation of privacy in their aggregated movements. Indeed, in today's world of satellite technology and the Internet, "[p]eople keep information about themselves private all the time without 'exhibiting' that interest in any perceptible way."[354] Individuals may maintain an expectation of privacy in their conversations, emails, or aggregated location information based on their own subjective understandings of privacy—whether legal, political, or philosophical—but display no conscious efforts to keep them private.[355] This is in part because they do not exist in physical form, and in part because expectations of privacy are rarely "explicit" or "exhibited," and are more often a part of habit or custom.[356]

Thus, determinations as to whether an individual has erected "No Trespassing" signs on his property or parked his vehicle in a private garage are not indicative of actual privacy interests.[357] How should a court treat the two-car family who parks one vehicle in their garage, and one in an exposed driveway (to say nothing of the city-dwelling family that parks on a public street)? Can we actually assume that the owners maintain varied expectations of privacy in their vehicles based on where they park them? Moreover, as Chief Judge Alex Kozinski noted in dissent to the denial of a rehearing of *Pineda-Moreno*, this type of reasoning necessarily demarcates subjective expectations of privacy on the basis of socio-economic factors such as income and housing.[358] Individuals who live inside gated communities will always be able to claim a clearly demonstrated expectation of privacy, while those who live in apartment buildings without garages will be unable demonstrate a similar expectation.[359] However, "the Constitution doesn't prefer the rich over the poor; the man who parks his car next to his trailer is entitled to the same privacy and peace of mind as the man whose

352. *See* Harper, *supra* note 60, at 1386.

353. United States v. Holmes, 521 F.2d 859, 865 (5th Cir. 1975), *aff'd en banc*, 537 F.2d 227 (1976).

354. *See* Harper, *supra* note 60, at 1386.

355. *See id.* at 1387.

356. *See id.*

357. *See supra* notes 171-172 and accompanying text; *see also* United States v. Sparks, No. 10-10067, 2010 WL 4595522, at *4 (D. Mass. Nov. 10, 2010) (reasoning that for a "modern urban multifamily apartment house," the area of the curtilage was "necessarily much more limited").

358. *See* United States v. Pineda-Moreno, 617 F.3d 1120, 1123 (9th Cir. 2010) (Kozinski, C.J., dissenting).

359. *Id.*; *see also supra* note 172 and accompanying text.

urban fortress is guarded by the Bel Air Patrol."[360] A continuation of this type of analysis would be an unfortunate turn in Fourth Amendment jurisprudence, tying Fourth Amendment protections indirectly to factors of race and class.

i. The Probabilistic Model[361]

An individual's subjective expectation of privacy in his movements twenty-four hours per day should not be derived from where he parks his car, but from whether or not this information has actually been "exposed" to anyone.[362] Under the D.C. Circuit's probabilistic analysis, whether something is exposed to the public depends not upon the theoretical possibility but upon the actual likelihood of discovery by a stranger.[363] In other words, while an individual may be aware of the technical possibility that someone may physically follow him twenty-four hours per day, for weeks or months at a time, the expectation that it will actually happen is "effectively nil."[364] Thus, an individual's subjective expectation that the government will not track him for four weeks,[365] sixty-five days,[366] or three months,[367] is both actual and reasonable.

Some courts have found this probabilistic analysis irrelevant because the Supreme Court has held certain government actions—rifling through a suspect's trash while it was placed on the curb,[368] or renting an airplane to conduct aerial surveillance[369]—to be constitutional regardless of whether the action was expected by the defendants.[370] However, the Supreme Court has indeed used probabilistic determinations in its calculation of whether a defendant has a reasonable expectation of privacy.[371] In *Bond v. United*

360. *Pineda-Moreno*, 617 F.3d at 1123 (Kozinski, C.J., dissenting).

361. For a discussion of probabilistic analysis, see *supra* note 117 and accompanying text.

362. *See supra* note 246 and accompanying text.

363. United States v. Maynard, 615 F.3d 544, 560 (D.C. Cir. 2010), *reh'g en banc denied sub nom.* United States v. Jones, 625 F.3d 766, *cert. denied*, Maynard v. United States, No. 10-7102, 2010 WL 4156203 (Nov. 29, 2010).

364. *Id.*

365. The duration of GPS surveillance in *Maynard*, 615 F.3d at 555.

366. The duration of GPS surveillance in *People v. Weaver*, 909 N.E.2d 1195, 1195 (N.Y. 2009).

367. The minimum duration of GPS surveillance in *United States v. Marquez*, 605 F.3d 604, 607 (8th Cir. 2010). *See supra* note 151.

368. California v. Greenwood, 486 U.S. 35, 40 (1988).

369. California v. Ciraolo, 476 U.S. 207, 215 (1986).

370. United States v. Sparks, No. 10-10067, 2010 WL 4595522, at *7 (D. Mass. Nov. 10, 2010).

371. *See supra* note 117.

States,[372] for example, the Supreme Court held that the squeezing of a bus passenger's luggage by a border patrol agent constituted a search because it exceeded what a reasonable bus passenger would expect in the handling of his luggage.[373] Moreover, in *California v. Ciraolo*,[374] while the Justices disagreed on the likelihood of aerial surveillance of a defendant's private property, both the majority and dissenting opinions agreed that the proper inquiry to determine reasonableness included the probability that the suspect's property would be subject to observation by others.[375]

ii. The Mosaic Theory

Courts have also challenged the probabilistic model in light of the Supreme Court's statement in *Jacobsen* that the concept of privacy is "critically different from the mere expectation . . . that certain facts will not come to the attention of the authorities."[376] However, GPS surveillance reveals much more than "certain facts." In fact, the quantitative and qualitative information gathered from the aggregation of an individual's location information over weeks or months can present an incredibly detailed view of an individual's life. Over the course of several weeks or months, individuals are guaranteed to pass through many different spheres, some of which they may subjectively consider more "private" than others, including places of worship, the doctor's office, and political clubs.[377] Because the sequence of a person's movements can reveal more than individual glimpses, the whole is worth much more than the sum of its parts.[378]

This detailed patchwork of information reveals the so-called "mosaic" of an individual's life—a profile not simply of where he goes, but also of his associations—the implications of which conjure the protections of the First Amendment as well as the Fourth.[379] In Supreme Court jurisprudence, where a search reveals "intimate details" of a private area, it deserves Fourth Amendment protection.[380] Given that this intimate view of an indi-

372. 529 U.S. 334 (2000).

373. *Id.* at 338-39.

374. 476 U.S. at 207.

375. *Id.* at 213-14, 223 (Powell, J., dissenting).

376. United States v. Jacobsen, 466 U.S. 109, 122 (1984). In *Jacobsen*, for example, "certain facts" referred to the fact that a white substance was in fact cocaine. *Id.*

377. *See supra* notes 224-228, 250-252 and accompanying text.

378. *See* United States v. Maynard, 615 F.3d 544, 562 (D.C. Cir. 2010), *reh'g en banc denied sub nom.* United States v. Jones, 625 F.3d 766, *cert. denied*, Maynard v. United States, No. 10-7102, 2010 WL 4156203 (Nov. 29, 2010); *see also supra* notes 250-252 and accompanying text.

379. *See* People v. Weaver, 909 N.E.2d 1195, 1199-1200 (N.Y. 2009).

380. *See* Kyllo v. United States, 533 U.S. 27, 37 (2001).

vidual's life may reveal even more details than if the government entered and searched his home, and especially in light of the fact that the Fourth Amendment protects "people, not places," obtaining this type of personal profile through GPS surveillance should require a warrant.[381]

While the government has argued that finding a search under the Mosaic Theory unconstitutional would also therefore prohibit twenty-four hour visual surveillance,[382] the Supreme Court has held that "[t]he fact that equivalent information could sometimes be obtained by other means does not make lawful the use of means that violate the Fourth Amendment."[383] For example, "the police might . . . learn how many people are in a particular house by setting up year-round surveillance; but that does not make breaking and entering to find out the same information lawful."[384] Thus, while visual surveillance of a suspect twenty-four hours per day would be constitutional, attaching a device that utilizes satellite technology to his personal vehicle to aggregate his location information and send it to a remote computer may still violate the Fourth Amendment.

Visual surveillance can be further differentiated from GPS surveillance because people generally understand that law enforcement may follow them on a street or in a car. They have sensory means of telling that they are being followed. Suspects can maneuver to keep themselves hidden, staying on the run for days or weeks at a time. If a person is following you, he is limited by human capabilities. If an electronic device is following you, its capabilities are nearly limitless.[385]

2. What Would Facebook Say? How Society Governs the Second Prong of Katz

The second prong of the *Katz* test asks whether an individual's actual expectation of privacy is "one that society is prepared to recognize as reasonable"[386]—or as the Court wrote in *Knotts*—"whether the person invoking [Fourth Amendment] protection can claim a 'justifiable,' a 'reasonable,' or a 'legitimate expectation of privacy' that has been invaded by government action."[387] If the government's position were correct, we would have to accept that twenty-four hour surveillance is now something

381. *See* Ottenberg, *supra* note 2186, at 661, 698 (citing Katz v. United States, 389 U.S. 347, 351-52 (1967)).

382. *See Maynard*, 615 F.3d at 565.

383. *Kyllo*, 533 U.S. at 35 n.2.

384. *Id.*

385. *See supra* notes 17-18 and accompanying text.

386. Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring) (internal quotation marks omitted).

387. United States v. Knotts, 460 U.S. 276, 280 (1983).

society recognizes as reasonable, even where there is no ability for individuals to detect when they are being scrutinized. This premise is "nothing short of a staggering limitation upon personal freedom,"[388] even in an age of increased public awareness and use of location technology. Indeed, public awareness and use of this type of technology has not translated to a diminution in privacy expectations. In fact, it is possible that we have begun to see an emergence of a trend solidifying some of these privacy interests in the age of Facebook and Google Street View.

i. The Effect of Public Awareness and Use of GPS Technology

The determination of "society's" opinion is complicated not only by its inherent circularity,[389] but by the newness of the "Information Age"—of Facebook, Google, iPhones, and Foursquare—because ideas of privacy within these mediums are still taking shape.[390] The result has been, as some commentators have described it, "a battle" to determine, and in turn define, societal expectations.[391] For example, the District Court in *Sparks* pointed to media coverage of GPS tracking by law enforcement in the investigation of Scott Peterson as evidence of public awareness of this practice, weighing against a defendant's claim of a reasonable expectation of privacy.[392] However, mere public knowledge of a certain practice indicates neither acceptance of that practice (especially where its legality is in question) nor a diminished expectation that they too will be tracked without a warrant. Indeed, as the Supreme Court reminded us in *Boyd v. United States*: "It may be that it is the obnoxious thing in its mildest and least repulsive form; but illegitimate and unconstitutional practices get their first footing in that way, namely, by silent approaches and slight deviations from legal modes of procedure."[393]

Courts have also alluded to the fact that increased public use of GPS technology could indicate a diminished expectation of privacy in an individual's movements. For example, in determining whether a violation of the Fourth Amendment occurred, the Supreme Court has looked at whether the technology was used by the public at large.[394] However, public use of

388. State v. Campbell, 759 P.2d 1040, 1048-49 (Or. 1988).

389. *See supra* notes 66-69 and accompanying text.

390. *See* Harper, *supra* note 60, at 1392.

391. *See id.*

392. *See* United States v. Sparks, No. 10-10067, 2010 WL 4595522, at *7 (D. Mass. Nov. 10, 2010) (citing *Judge Allows GPS Evidence in Peterson Case*, CNN.COM (Feb. 17, 2004), http://www.cnn.com/2004/LAW/02/17/peterson.trial/index.html).

393. Boyd v. United States, 116 U.S. 616, 635 (1886).

394. *See* Kyllo v. United States, 533 U.S. 27, 34 (2001); Dow Chemical Co. v. United States, 476 U.S. 227, 246-47 (1986).

or familiarity with a certain technology does not indicate that it is per se reasonable under the Fourth Amendment. The recent decision by the Third Circuit allowing magistrate judges to require warrants for historical CSI demonstrates that even technology as ubiquitous as cell phone technology can still implicate the Fourth Amendment.[395] Indeed, simply because a private company can access information in the content of emails or through cell phones, "the privacy expectation in the content of either is not diminished, because there is a societal expectation that the ISP or the phone company will not do so as a matter of course."[396]

Rather, despite the increasing use of GPS technology, there is no evidence of a "corresponding societal expectation that government authorities will use such devices to track private citizens."[397] The Reddit.com community certainly did not appear to understand or accept as reasonable the government's attachment and monitoring of a tracking device to the California student's car.[398] And despite the District Court's attempt in *Sparks* to glean public knowledge and acceptance of these practices from media reports,[399] even a cursory survey of recent headlines regarding warrantless government tracking, either by vehicle or cell phone, reveals that awareness of GPS and CSI surveillance has not resulted in acquiescence or a diminished expectation of privacy.[400] In fact, it appears that just the opposite is true, as the myriad articles in newspapers, magazines, and blogs describing the practice have also noted the attendant controversy and concern. For example, a February 2010 *Newsweek Magazine* article described cell phone tracking as "among the more unsettling forms of government surveillance, conjuring up Orwellian images of Big Brother," suggesting that most of the nation's 277 million cell phone users "don't have a clue" that the government could track them through their cell phones.[401] Editorial boards from the *New York Times* to the *Utah Daily Herald* have opined in favor of requiring a warrant for GPS tracking of vehicles.[402] National Public Radio

395. *See In re* Order Directing a Provider of Elec. Commc'n Serv. to Disclose Records to the Gov't, 620 F.3d 304, 319 (3rd Cir. Sept. 7, 2010).

396. *Orenstein Opinion*, *supra* note 279, at *28.

397. Commonwealth v. Connolly, 913 N.E.2d 356, 369 (Mass. 2009).

398. *See supra* notes 8-10 and accompanying text.

399. *See supra* notes 192-195 and accompanying text.

400. *See infra* notes 401-403 and accompanying text.

401. Michael Isikoff, *The Snitch in Your Pocket*, NEWSWEEK, Feb. 19, 2010, http://www.newsweek.com/2010/02/18/the-snitch-in-your-pocket.html; *see also supra* note 320.

402. *See* Editorial, *GPS and Privacy Rights*, N.Y. TIMES, May 14, 2009, http://www.nytimes.com/2009/05/15/opinion/15fri3.html?scp=3&sq=gps%20tracking%20vehicle%20weaver&st=cse; Editorial, *Shun Warrantless GPS Tracking*, UTAH DAILY HERALD (Sept. 16, 2010, 12:09 AM), http://www.heraldextra.com/news/opinion/editorial/article_5e731cb9-5fef-5dc3-96a5-dc5dfc3cb8a1.html.

produced a story on the Reddit.com student, noting the fear and anger caused by the FBI's actions.[403]

ii. Recent Privacy Invasions Produce a Demand for Greater Control

In fact, public awareness of certain technological invasions of privacy has in some cases produced an increasing demand for control.[404] General suggestions that, in the current climate of "over-sharing" on Facebook, MySpace, and Twitter, Americans have acquiesced to "the end of privacy,"[405] have been refuted by a number of recent events which reflect a growing trend towards maintaining and protecting privacy rights in an age of rapidly-evolving technology. Facebook, which has been embroiled in several privacy concerns since its inception over the use of its members' personal information, experienced another uproar in October 2010, after a *Wall Street Journal* investigation found that users' identification information was being transmitted to third parties via Facebook applications.[406] In response to the controversy, Facebook took steps to "dramatically limit" the exposure of personal information and created a Facebook "Bill of Rights and Responsibilities."[407] Google's endeavor to record 360-degree images of street corners throughout the world resulted in lawsuits and an FCC investigation after it became clear that the company had also collected personal information over wireless Internet networks in the process.[408] Meanwhile, public furor and a class action lawsuit over "Google Buzz" literally shut down the company's first attempt to enter the social networking realm, after it became clear that they had added "followers" to users' accounts without first asking permission.[409] It was this type of controversy

403. 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. The student is now represented by an attorney at the Bay Area branch of the Council on American-Islamic Relations. *Id.*

404. *See Orenstein Opinion*, *supra* note 279, at *46; *see also infra* notes 406-413 and accompanying text.

405. CNN's term for the recent explosion in Internet sharing. *See* Sutter, *supra* note 137.

406. Emily Steele & Geoffrey A. Fowler, *Facebook in Privacy Breach*, WALL ST. J., Oct. 18, 2010, http://online.wsj.com/article/SB10001424052702304772804575558484075236968.html.

407. *See id.*; Press Release, Facebook, Facebook Opens Governance of Service and Policy Process to Users (Feb. 26, 2009), *available at* http://www.facebook.com/press/releases.php?p=85587.

408. Edward Wyatt, *F.C.C. Investigates Google Street View*, N.Y. TIMES, Nov. 10, 2010, http://www.nytimes.com/2010/11/11/technology/11google.html?_r=1.

409. Rob Spiegel, *Google Puts Buzz Privacy Flap to Rest*, E-COMMERCE TIMES (Nov. 3, 2010, 11:20 AM), http://www.technewsworld.com/story/71167.html?wlc=1289008958.

that caused *Business Week* to declare that contrary to popular belief, "Gen Yers" were just as concerned about their privacy as their parents.[410]

Meanwhile, the Federal Trade Commission released a report in December 2010 calling for more transparency in how websites use the information they collect and for users to be able to opt out of having their personal data mined and shared with advertisers.[411] The report even cited to the D.C. Circuit's decision in *United States v. Maynard* for its proposition that compilation of electronic data "poses different and more substantial privacy risks than collection of information regarding a discrete incident, because it offers the ability to obtain an intimate picture of an individual's life."[412] The U.S. Congress is considering a "Do-Not-Track" option for Internet surfing that would operate similarly to the Do-Not-Call list blocking telemarketers.[413] Several state legislatures, including California, Hawaii, South Carolina, and Minnesota have passed statutes codifying the warrant requirement for use of tracking devices by the government.[414] In December 2010, the Sixth Circuit ruled that the government must obtain a search warrant before seizing and searching emails stored by email service providers, marking the first time a federal appeals court has explicitly extended the Fourth Amendment's warrant requirement to email.[415] Commenting on the case, Professor Jonathan Askin of Brooklyn Law School noted that these cases demonstrate that although the framers of the Constitution may not have been able to consider modern modes of communication, this "does not mean that government gets a free pass to intercept and listen in without following constitutionally mandated process."[416]

410. Bruce Nussbaum, *Facebook Privacy Flap—Gen Yers Demand Control*, BUS. WK. (Feb. 18, 2009), http://www.businessweek.com/innovate/NussbaumOnDesign/archives/2009/02/facebook_privacy_flap--gen_yers_demand_control.html) ("For a while there, it seemed that Gen Y believe in a No-Privacy rule and didn't care who owned the numbers in their lives. . . . The uproar over Facebook's new policy on ownership of peoples' posts . . . shows the contrary.").

411. FED. TRADE COMM'N, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE: A PROPOSED FRAMEWORK FOR BUSINESSES AND POLICYMAKERS (2010), *available at* http://www.ftc.gov/os/2010/12/101201privacyreport.pdf.

412. *See id.* at 21 (citing United States v. Maynard, 615 F.3d 544, 556-64 (D.C. Cir. 2010)).

413. Jim Puzzanghera, *'Do not Track' Bill to Protect Online Privacy Worries Some Lawmakers*, L.A. TIMES BLOG (Dec. 2, 2010, 1:59 PM), http://latimesblogs.latimes.com/technology/2010/12/do-not-track-privacy-online-ads-federal-trade-commission-congress.html.

414. *See supra* note 254.

415. *See* United States v. Warshak, Nos. 08-3997, 08-4212, 08-4085, 08-4429, 08-4087, 09-3176, 2010 WL 5071766, at *1 (6th Cir. Dec. 14, 2010).

416. Erika Morphy, *Court Ruling Grants Email the Cloak of Privacy*, E-COMMERCE TIMES (Dec. 15, 2010), http://www.ecommercetimes.com/story/71467.html?wlc=1292480037.

Ultimately, it is no longer sufficient to analogize twenty-four hour GPS surveillance to following a vehicle on public roads. The battle that has broken out over GPS and cell phone surveillance—among privacy advocates, judges, government, and the media—indicates that this type of action constitutes something much greater. Indeed, "George Orwell's *1984* would not retain its emotive power if people did not believe that they enjoy freedom from extensive, around-the-clock technological tracking."[417] Thus, for the sake protecting the significant privacy interests that are clearly still considered legitimate by our society, this "split" should be resolved in favor of a warrant.

D. One Standard for All: Preserving Consistency in the Warrant Requirement

GPS surveillance may very well be the most effective, efficient and inexpensive way to conduct surveillance; in fact, no one is saying the government is prohibited from doing it. Rather, all that is being asked is that the government obtain a warrant based on probable cause in order to maintain judicial supervision over a practice that is ripe for abuse. As noted in Part I, from a practical perspective, the Fourth Amendment essentially functions as a procedural requirement; rather than prohibiting searches and seizures all together, it requires that law enforcement obtain a warrant based on probable cause.[418] The historical judgment encapsulated by the Fourth Amendment was that unlimited discretion among those with investigatory and prosecutorial duties would produce pressure to "overlook potential invasions of privacy."[419] Even the Supreme Court has made it abundantly clear that it still considers judicial oversight over government surveillance necessary to prevent abuse by law enforcement;[420] in *Karo*, the Court found the government's argument that warrantless beeper searches should always be "reasonable" to be based upon "its deprecation of the benefits and exaggeration of the difficulties associated with procurement of a warrant."[421] Instead, the Court wrote, warrants are necessary in guaranteeing that tracking devices are not abused, "by imposing upon agents the requirement that they demonstrate in advance their justification for the desired search."[422]

417. Brief of *Amici Curiae* Electronic Frontier Foundation and American Civil Liberties Union of the National Capital Area in Support of Appellant Jones at 22, United States v. Maynard, 615 F.3d 544 (D.C. Cir. 2010); *see also* ORWELL, *supra* note 320.

418. *See* Kothari, *supra* note 40, at 8.

419. United States v. U.S. Dist. Ct., 407 U.S. 297, 317 (1972).

420. United States v. Karo, 468 U.S. 705, 717 (1984).

421. *Id.*

422. *Id.*

In addition to the need for judicial supervision, GPS surveillance should require a warrant in the interest of consistency and equal application of our laws. A closer inspection reveals that the case law regarding GPS surveillance is far from clear. While the Seventh, Eighth, and Ninth Circuits have held that GPS surveillance does not require a warrant,[423] the Eighth Circuit required an intermediate showing of "reasonable suspicion" to justify use of the tracking device.[424] Meanwhile, other circuits to consider the earlier form of beeper surveillance—including the First, Fifth, and Tenth Circuits—have similarly required varied showings of cause, from reasonable suspicion to probable cause, even in absence of a warrant requirement.[425] Thus, current Fourth Amendment law in fact contains a medley of standards for tracking devices, which is further complicated by the parallel standards being applied for cell phone surveillance.[426] From this chaos, however, one thing is clear: it would not make legal or rational sense to allow two divergent standards for twenty-four hour electronic surveillance of citizens. Dismissing GPS surveillance as neither search nor seizure would allow twenty-four hour tracking of citizens through their vehicles with no requirement of probable cause,[427] while similar prospective (and perhaps even historical) tracking through cell phones would require a warrant.[428] In the interest of consistency, efficiency, and protection against abuse, there should be one standard for twenty-four hour government surveillance by vehicle or by cell phone. In light of the implications discussed above, this standard should be a warrant based on probable cause.

CONCLUSION

Concerns over government intrusion into individual privacy are not new; rather, the historical context surrounding the Bill of Rights demonstrates that the Fourth Amendment was not merely a shield against the government entering a person's house—it was a protection against government intrusion more generally.[429] Perhaps this is why even those courts that have allowed for warrantless GPS surveillance have noted with caution that this technology "enable[s], as the old (because of expense) do not, wholesale surveillance."[430] The court in *Sparks* even warned: "although we are not

423. *See supra* Part II.A.
424. *See* United States v. Marquez, 605 F.3d 604, 610 (8th Cir. 2010).
425. *See supra* note 91.
426. *See supra* Part II.C.
427. *See supra* Part II.A.
428. *See supra* notes 275-279 and accompanying text.
429. *See* Kothari, *supra* note 40, at 6.
430. United States v. Garcia, 474 F.3d 994, 998 (7th Cir. 2007).

yet faced with police overreaching, it may very well be near, and this Court and others will be keeping vigilant watch."[431]

Indeed, at the heart of this debate lies a deep-seated uneasiness with governments conducting surveillance of their citizens. These hesitancies belie a political caution which attends government surveillance and has refused to vanish from our societal conscience: "There is something creepy and un-American about such clandestine and underhanded behavior," wrote Chief Judge Alex Kozinski, dissenting from the denial of Pineda-Moreno's rehearing.[432] "To those of us who have lived under a totalitarian regime, there is an eerie feeling of déjà vu."[433] While trust in the national government waxes and wanes, and technology continually introduces new means of mining the personal preferences of every citizen, our laws should remain steadfast in their protections. Allowing GPS surveillance without any judicial supervision would represent a giant step backward in this nation's approach to individual freedoms.

431. United States v. Sparks, No. 10-10067, 2010 WL 4595522, at *10 (D. Mass. Nov. 10, 2010).

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

433. *Id.*