LOCATING LOCATION PRIVACY

David H. Goetz†

The Fourth Amendment protects citizens of the United States from unreasonable search or seizure.[1] The framers of the Constitution enacted the Fourth Amendment to curb the government's power to interfere with a citizen's right to keep his private life hidden from government view.[2] Specifically, the framers did not trust that a government unchecked in its ability to peer into its citizens' private lives would wield that power judiciously.[3] At the same time, the government must also balance this privacy interest against the public's interest in peace and security, which may be served through the gathering of evidence and enforcement of law.[4]

Today, this balancing between privacy protection and law enforcement must also consider the growing ability of the government to use technology to peer into the private lives of individuals. Consider the cellular telephone and the global positioning system (GPS) device. The government at both the local and national level is increasingly seeking routine access to location information derived from cell phone and GPS devices.[5] In the case of cell phones, the government can request both real time and historical information related to a cell phone's location from a service provider without

---

† J.D. Candidate, 2012, University of California, Berkeley School of Law.

1. U.S. CONST. amend. IV ("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.").

2. THOMAS N. MCINNIS, THE EVOLUTION OF THE FOURTH AMENDMENT 4 (2009) ("To help ensure that there will be limits on the power of the American government to arbitrarily interfere in the lives of its citizens the first Congress proposed and in 1791 the states ratified the Fourth Amendment to the Constitution.").

3. Boyd v. United States, 116 U.S. 616, 641 (1886) ("[T]he framers of the Constitution had their attention drawn, no doubt, to the abuses of this power of searching private houses and seizing private papers . . . .").

4. *See, e.g.*, United States v. Place, 462 U.S. 696, 703 (1983) ("We must balance the nature and quality of the intrusion on the individual's Fourth Amendment interests against the importance of the governmental interests alleged to justify the intrusion.").

5. Michael Isikoff, *The Snitch in Your Pocket Law Enforcement Is Tracking Americans' Cell Phones in Real Time—Without the Benefit of a Warrant*, NEWSWEEK, Mar. 1, 2010, at 40 ("[C]ompanies are now getting 'thousands of these requests per month,' and the amount has grown 'exponentially' over the past few years.").

a warrant.[6] In the case of GPS devices, law enforcement agencies in many jurisdictions may attach them to a private citizen's vehicle without a warrant and track the movements of that vehicle continuously and for months at a time.[7] As the state becomes increasingly able to gather and use information on its citizens, some argue that there is a risk that the government will be able to monitor and control vast areas of private life.[8] Others argue, however, that because modern crimes have become increasingly complex, there is a greater need for the government to access personal information in the pursuit of its peace-keeping and law enforcement duties.[9]

This Note addresses the imbalance between the public's interest in privacy protection and law enforcement's interest in evidence gathering activities resulting from the rise of facile electronic communication and surveillance technologies, specifically GPS tracking.[10] It argues that warrantless and continuous tracking by law enforcement is an encroachment on basic Fourth Amendment rights due to the intrusive and private nature of the information thus obtained, information that could never be obtained by more traditional methods.[11] This Note distinguishes government surveillance

---

6. *In re* United States for Order for Disclosure of Telecomm. Records, 405 F. Supp. 2d 435, 449 (S.D.N.Y. 2005) (holding that warrantless access to cell site location information by the government is not a violation of the Fourth Amendment). *But see In re* United States *ex rel.* Historical Cell Site Data, No. H-10-998M, 2010 WL 4286365, at *14 (S.D. Tex. Oct. 29, 2010) (holding that warrantless access by the government to cell site location information is a violation of the Fourth Amendment).

7. United States v. Maynard, 615 F.3d 544, 549 (D.C. Cir. 2010); United States v. Pineda-Moreno, 591 F.3d 1212, 1213 (9th Cir. 2010); United States v. Marquez, 605 F.3d 604, 607 (8th Cir. 2010); United States v. Garcia, 474 F.3d 994, 995 (7th Cir. 2007); Mina Kim, *FBI's GPS Tracking Raises Privacy Concerns*, NPR (Oct. 27, 2010), http://www.npr.org/templates/story/story.php?storyId=130833487.

8. Katherine Strandburg, *Freedom of Association in a Networked World: First Amendment Regulation of Relational Surveillance*, 49 B.C. L. REV. 741, 747 (2008) ("The potential chilling effect [of government] surveillance poses serious risks . . . to individual privacy").

9. *See, e.g.*, Christopher Nolin, *Telecommunications as a Weapon in the War of Modern Organized Crime*, 15 COMMLAW CONSPECTUS 231, 242–45 (2007) (describing the necessary use of technological means by law enforcement to intercept communications to combat the increasingly complex criminal schemes perpetrated by organized crime).

10. To be sure, such balancing between regulating the government's use of intrusive surveillance technologies and protecting its citizens is not limited to the use of GPS tracking devices. Consider, for example, the privacy issues at stake during routine airport screening in the age of backscatter X-ray and mm wave radar scanners capable of seeing through a person's clothes.

11. For example, it is commonly assumed that GPS and cell phone tracking merely make it easier for the government to follow or track a person around during his public travel. However, as this Note will make clear, no law enforcement agency in the United States has the ability to follow even a single individual day and night for months on end

using a GPS tracking device that is limited in duration and scope from the continuous drag-net type surveillance that represents an abuse of governmental power.

Part I provides a brief historical overview of information privacy law relating to the use of surveillance technology, with an emphasis on how the courts have addressed the ability of advancing technology to peer into the private lives of citizens. Part II provides a brief overview of cell phone and GPS technologies. This Part examines how these technologies differ from each other and how these differences affect the government's access to the location information they produce. Part III contrasts three cases in which the courts find that warrantless GPS tracking is not a Fourth Amendment violation with the recent District of Columbia Circuit opinion that places important limits on the ability of the government to engage in unlimited warrantless GPS tracking. Part IV then proposes application of the D.C. Circuit's totality of the information (TOI) theory to warrantless GPS tracking by law enforcement agencies and shows how this legal theory is consistent with historical Fourth Amendment jurisprudence.

I. PRIVACY LAW AND SURVEILLANCE TECHNOLOGY

The Fourth Amendment is the foundation that protects citizens' privacy interests from government intrusion. Accordingly, this Part reviews important milestones in Fourth Amendment jurisprudence with emphasis on how the courts have dealt with the emergence of new surveillance technologies.

The Fourth Amendment provides that "[t]he 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."[12] In the context of the Fourth Amendment, a search is the act of looking for a person or gathering evidence of a crime by a law enforcement officer in a place where a citizen has a reasonable expectation of privacy.[13] In contrast, a seizure is the act of taking possession of a person or object by an officer.[14]

without ever losing contact. Therefore, these technologies do provide information that could never be obtained by traditional police surveillance methods.

12. U.S. CONST. amend. IV.

13. *See* Hale v. Henkel, 201 U.S. 43, 80 (1906) ("[A] search implies a quest by an officer of the law; a seizure contemplates a forcible dispossession of the owner.").

14. *See id.*

But in practice, many Fourth Amendment cases fail to distinguish between searches and seizures.[15]

Although the Fourth Amendment does not explicitly require a warrant for the government to search a citizen's persons or effects, courts have interpreted the Fourth Amendment as providing a default warrant requirement.[16] Searches and seizures performed by law enforcement without a warrant are presumptively unreasonable, and, absent consent or exigent circumstances, are thus unconstitutional.[17] The remedy for evidence held to have been obtained by an illegal search or seizure is to exclude that evidence from use at trial.[18]

The courts, however, have not laid out any specific test for identifying whether exigent circumstances exist.[19] Traditionally, courts have recognized a narrowly limited number of exigent circumstances that allow warrantless

15. *See, e.g.*, *Ex parte* Jackson, 96 U.S. 727, 733 (1878) (holding that the sealed contents of postal mail may not be searched or seized); *But see* United States v. Garcia, 474 F.3d 994, 996–97 (7th Cir. 2007) (separately holding that tracking a suspect's vehicle with an electronic device was not a search, and that attaching said tracking device to the vehicle was not a seizure).

16. *See, e.g.*, Mincey v. Arizona, 437 U.S. 385, 390 (1978) (holding that a search conducted without a warrant is per se unreasonable under the Fourth Amendment).

17. Johnson v. United States, 333 U.S. 10, 14–15 (1948) ("There are exceptional circumstances in which, on balancing the need for effective law enforcement against the right of privacy, it may be contended that a magistrate's warrant for search may be dispensed with."); *see, e.g.*, Schneckloth v. Bustamonte, 412 U.S. 218 (1973) (consent); Warden v. Hayden, 387 U.S. 294, 298 (1967) (exigent circumstances).

18. Weeks v. United States, 232 U.S. 383, 398 (1914) (holding that the use of evidence obtained in violation of the Fourth Amendment at trial is prejudicial error). The underlying rationale for this exclusion doctrine is to deter law enforcement from violating the Fourth Amendment in the future, rather than to remedy the past violation, thus exclusion is not provided in all circumstances in which a violation has been found. Tony D. Tague, *Good Faith and the Exclusionary Rule: Demise of the Exclusion Illusion*, 30 AM. U. L. REV. 863, 871 (1980) ("Although the Court did not explicitly mention the deterrent rationale in the early stages of the exclusionary rule's development, the more recent cases establish the deterrence theory as the prominent justification for inclusion of the exclusionary rule in modern criminal procedure.").

19. *See generally* Chimel v. California, 395 U.S. 752, 755-60 (1969) (reviewing precedent for the exceptional circumstances doctrine); Warden v. Hayden, 387 U.S. 294, 298–300 (1967) (holding that a search of a home into which a suspected armed felon has just entered is reasonable under the circumstances); Cooper v. California, 386 U.S. 58, 61–62 (1967) (holding that police may search an impounded automobile without a warrant if the search is closely related to the reason the automobile was impounded); Brinegar v. United States, 338 U.S. 160, 174–77 (1949) (holding that evidence may be considered at a probable cause hearing that should be excluded at trial); McDonald v. United States, 335 U.S. 451, 454–56 (1948) (holding that in the absence of an emergency or other compelling reason, a warrant is required to search a home); Carroll v. United States, 267 U.S. 132, 153, 156 (1925) (establishing automobile exception).

searches. For example, automobiles, because of their inherent mobility, are subject to warrantless searches. [20] Therefore, officers need not obtain a warrant to perform a search of an automobile incident to a lawful arrest in the dual interests of safety and preservation of evidence.[21]

The Supreme Court has also held that a warrant must be based on probable cause determined by a neutral magistrate.[22] The requirement for a neutral magistrate interposes a disinterested party trained in the meaning of probable cause and exigency between the government's desire to gather evidence and a citizen's right to privacy. It is important to note that the cases discussed below involve the Court's determination whether the police's *warrantless* surveillance of individuals using technology violated the Fourth Amendment. This Note does not consider the government's use of technology to surveil individuals when they have a warrant, as these activities are considered per se reasonable absent some evidence that the warrant was not issued by a neutral magistrate[23] or was otherwise invalid.[24]

The threshold question for whether the Fourth Amendment applies is whether there was an actual search or seizure by the government (e.g., law enforcement).[25] Although a plain meaning analysis of the Amendment itself might suggest that all information gathering activities by the government are subject to Fourth Amendment protection, case law holds that the use of technology by law enforcement to observe illicit activity or gather evidence may not constitute a search cognizable under the Constitution if such information was not held away from the public view.[26]

Early decisions regarding the use of technology and Fourth Amendment considerations focused on whether there had been a physical intrusion into a

---

20. *Caroll*, 267 U.S. at 156 (although probable cause is still necessary to support a search under the Fourth Amendment).

21. *Chimel*, 395 U.S. 752.

22. United States v. Jeffers, 342 U.S. 48, 52 (1951); United States v. Lefkowitz , 285 U.S. 452, 464 (1932).

23. Coolidge v. New Hampshire, 403 U.S. 443, 449–51 (1971) (invalidating warrant issued by state attorney general leading investigation).

24. Aguilar v. Texas, 378 U.S. 108, 113 (1964) (holding that officer's warrant issued by the magistrate judge was invalid because the "mere conclusion" that the suspect possessed narcotics presented in the officer's affidavit was not enough to support a finding of probable cause sufficient to support a valid warrant).

25. *See, e.g.*, United States v. Kyllo, 533 U.S. 27, 31 (2001) (characterizing the question of whether a search cognizable under the Fourth Amendment has occurred as an "antecedent question."); Dow Chem. Co. v. United States, 476 U.S. 227, 239 (1986) ("The taking of aerial photographs . . . is not a search prohibited by the Fourth Amendment.").

26. *See* California v. Ciraolo, 476 U.S. 207 (1986) (analyzing law enforcement's aerial observation under Fourth Amendment plain view doctrine and finding that observation of items in plain view is not a search subject to Fourth Amendment protections).

person's personal effects or their home.[27] In *Olmstead v. United States*, for example, the Court focused on the fact that officers did not penetrate defendant's house when using wire tapping equipment without a warrant to intercept phone calls and found that a violation of the Fourth Amendment had therefore not occurred because there was no search.[28] The Court's interpretation in *Olmstead* of the Fourth Amendment implications of wire tapping remained the law of the land for thirty-nine years.

However, in *Katz v. United States*, the Court overturned this approach.[29] Justice Stewart, writing for the majority, held that the Fourth Amendment "protects people, not places."[30] The Court extended Fourth Amendment protection against warrantless electronic eavesdropping on conversations held in a phone booth.[31] In doing so, the majority in *Katz* paid deference to the role of advancing technology in society and how our expectations of privacy may shift in response, finding that to hold that the Constitution was not meant to protect telephone conversations "is to ignore the vital role that the public telephone has come to play in private communication."[32]

In response to *Katz*, the courts have adopted the two-prong rule articulated in Justice Harlan's concurrence to determine whether or not a search subject to Fourth Amendment protection has occurred.[33] The first prong, whether the person exhibits a subjective expectation of privacy, is subject to a fact-based inquiry into the mind of the person searched.[34] The second prong is an objective test that asks whether that expectation is one that society is prepared to accept as reasonable.[35] This second prong is

27. Olmstead v. United States, 277 U.S. 438, 466 (1928) (holding that wiretapping of defendant's phone conversations from outside the home does not constitute a search as there has been no physical intrusion onto the defendant's person or property). *But see* Silverman v. United States, 365 U.S. 505, 510–12 (1961) (finding that officers' use of a "spike mike" to penetrate the home and listen to conversations therein constituted a violation of the Fourth Amendment although the intrusion was minor).

28. 277 U.S. at 464.

29. 389 U.S. 347, 353 (1967)

30. *Id.* at 351.

31. *Id.* at 351–53 (concluding that the holding in *Olmstead* was "so eroded by our subsequent decisions that the 'trespass' doctrine there enunciated can no longer be regarded as controlling"); *see also* Berger v. New York, 388 U.S. 41, 44 (1967) (striking down New York's eavesdropping laws authorizing warrantless electronic surveillance).

32. *Katz*, 389 U.S. at 351–53.

33. *Id.* at 361 (Harlan, J., concurring) (reasoning that Fourth Amendment protection rests on whether "first . . . a person ha[s] exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as 'reasonable.' ").

34. *Id.*

35. *Id.*

subject to a greater degree of fact-based inquiry because it considers not only whether society is prepared to accept the nature of the evidence gathering activity as reasonable, but also whether it is prepared to accept the nature of the obtained information as reasonable.[36] Combined, the two-prong test asks whether the information obtained is information that, except for the unreasonably intrusive activity by the government, would be private information. This two-pronged approach has lead to an unpredictable set of doctrines regarding how to treat information obtained using emerging surveillance technologies because the test relies on the Court's shifting expectations regarding exactly what activities and information society reasonably expects to be secure from government intrusion.[37]

One such doctrine is the third-party doctrine, which provides that any information willingly handed over to a third party is considered not subject to a reasonable expectation of privacy.[38] This doctrine stems from the Court's decision in *Smith v. Maryland*, which held that the warrantless use of a so-called pen register device installed at the telephone switching station, for recording the phone numbers dialed by an individual, did not violate the Fourth Amendment because the information was willingly conveyed to a third party—in this case, the phone company.[39]

Smith reveals the Court's concern with distinguishing between "content" and "address" or "envelope" information. In the much earlier case of *Ex parte Jackson*, the Court held that the contents of first class mail were entitled to Fourth Amendment protection, whereas the information written on the outside of the envelope or on a postcard had been willingly conveyed to the public and was not subject to such protection.[40] In the context of pen register surveillance in *Smith*, the Court emphasized that unlike the recording device in *Katz*, which recorded actual phone conversations, the pen register in *Smith* only recorded phone numbers which the Court considered distinguishable

36. Smith v. Maryland, 442 U.S. 735, 741 (1979) ("In applying the Katz analysis . . . it is important to begin by specifying precisely the nature of the state activity that is challenged.").

37. *See* Orin S. Kerr, *The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution*, 102 MICH. L. REV. 801, 826–27 (2004) ("Indeed, scholars consistently denounce the Court's opinions interpreting Katz as 'dead wrong,' 'off the mark,' 'misguided,' and 'inconsistent with the spirit of the fourth amendment.' ").

38. United States v. Miller, 425 U.S. 435, 443 (1976) (holding that defendant had no legitimate expectation of privacy in his bank records because the bank was a third party to which he voluntarily handed his information).

39. 442 U.S. at 741.

40. 96 U.S. 727, 733 (1878) ("[E]xcept as to their outward form and weight . . . [w]hilst in the mail, [letters and sealed packages] can only be . . . examined under like warrant, issued upon similar oath or affirmation, particularly describing the thing to be seized, as is required when papers are subjected to search in one's own household.").

from content.[41] However, the reasoning in *Smith* is not entirely consistent with the Court's holding in *Katz*. For example, unlike the envelope information in *Jackson*, the phone numbers dialed by *Smith* were not conveyed to any member of the public who wished to view the outside of the envelope; rather, the numbers were conveyed to the telephone company, and telephone companies do not provide information about the numbers a person has dialed to the public at large.

Another unpredictable doctrine is the Court's differentiation between surveillance technology used to track a person's activities in public versus a person's activities within his home. In *United States v. Knotts*, for example, the Court considered the warrantless use of a "beeper"[42] by law enforcement officers to track the movement of contraband.[43] The police placed the beeper inside a container of chloroform and tracked the chloroform from the place of purchase to the defendant's remote cabin.[44] The Court held that this type of tracking was not a search, in part, because the officers did not use the beeper to determine any information about the inside of the suspect's home.[45] The Court emphasized that a person's movements on a public thoroughfare are not subject to a reasonable expectation of privacy;[46] since the beeper merely enhances an officer's pre-existing ability to visually track such public movements,[47] it is not a search and thus not subject to Fourth Amendment protection.[48]

Importantly, the Court explicitly left open the question of whether "dragnet-type law enforcement activities," such as "twenty-four hour surveillance of any citizen of this country without judicial . . . supervision," might violate the Fourth Amendment.[49] The defendants argued that allowing warrantless use of a beeper device might allow continuous surveillance of a

41. *Smith*, 442 U.S. at 743 ("Although petitioner's conduct may have been calculated to keep the contents of his conversation private, his conduct was not and could not have been calculated to preserve the privacy of the number he dialed.").

42. A beeper is a device that emits a periodic electromagnetic signal that can be tracked by officers in proximity using a radio receiver. United States v. Knotts, 460 U.S. 276, 277 (1983).

43. *Id.*

44. *Id.*

45. *Id.* at 285 ("[T]here is no indication that the beeper was used in any way to reveal information as to the movement of the drum within the cabin, or in any way that would not have been visible to the naked eye from outside the cabin.").

46. *Id.* at 281.

47. *Id.* at 284 ("[B]eepers are merely a more effective means of observing what is already public.").

48. *Id.*

49. *Id.* at 283.

suspect without judicial supervision.[50] But the Court responded that such "dragnet-type" surveillance was not at issue in the case at hand, and therefore the Court need not address it.[51] Unfortunately, as explained, *infra* Part III, it is precisely this type of warrantless, twenty-four-hour extended surveillance that many courts now hold is acceptable under *Knotts* because these courts have erroneously equated the "dragnet-type" language in *Knotts* with wholesale surveillance, rather than the continuous twenty-four hour surveillance that the Court actually discussed.[52] Had the Court been addressing twenty-four-hour surveillance of every citizen, or a large number of citizens, or indiscriminate surveillance, or wholesale surveillance, then perhaps the subsequent interpretation of the Seventh, Eighth, and Ninth Circuit courts in applying *Knotts* to GPS tracking would be warranted. However, the text indicates that in reserving the question of "dragnet-type" surveillance, the Court was not reserving the question of wholesale warrantless surveillance of a large proportion of the citizenry; rather, it was reserving the question of whether prolonged and uninterrupted warrantless surveillance of *any* citizen implicates the Fourth Amendment.

In a later case, the Supreme Court put some limits on the warrantless use of electronic tracking devices. In *United States v. Karo*, law enforcement officers used a beeper without a warrant to determine the presence of contraband inside the private home of the suspect.[53] The Court held that the warrantless use of a tracking beeper to determine the presence or absence of an item in the home constituted a search and violated the Fourth Amendment.[54] The Court was not persuaded by the government's argument that the information provided by the beeper about the suspect's home was very limited, reasoning that nevertheless, the information provided by the beeper could not otherwise have been obtained without a lawful search pursuant to a warrant supported by probable cause.[55] Although the beeper in

50. *Id.*

51. *Id.* at 283–84.

52. *See, e.g.*, United States v. Pineda-Moreno, 591 F.3d 1212, n. 2 (9th Cir. 2010) (holding that under *Knotts*, prolonged and continuous surveillance without a warrant is not a Fourth Amendment violation).

53. 468 U.S. 705, 708 (1984).

54. *Id.* at 718; *cf. Knotts*, 460 U.S. 276, 285 (holding that when officers ceased tracking the electronic beeper device before it entered the suspect's home, the Fourth Amendment was not violated).

55. *Karo*, 460 U.S. at 714–15 ("[P]rivate residences are places in which the individual normally expects privacy free of governmental intrusion not authorized by a warrant, and that expectation is plainly one that society is prepared to recognize as justifiable. . . . [T]he monitoring indicated that the beeper was inside the house, a fact that could not have been visually verified.").

Karo was tracked for approximately five months, the Court declined to find that this type of prolonged warrantless surveillance was itself a Fourth Amendment violation, although the Court did note that the beeper was not tracked *continuously* during the five-month period.[56]

Taken together, *Knotts* and *Karo* are generally understood to mean that the government is free to place a tracking device on a suspect's car without a warrant and track the suspect's movements on public roads, but cannot obtain information about a suspect's home from such a device without a warrant.[57] This is illogical because suspects who store their vehicles in an attached garage are therefore safe from tracking devices since law enforcement officers fear that obtaining illegal information about the home will taint any legal information obtained, whereas suspects who park their vehicles on the street may be subject to warrantless tracking without limit.[58] Such reasoning has even been extended by some law enforcement agencies to the use of GPS tracking devices, even though they generally cannot operate indoors.[59]

The Court has also distinguished between technology that is publicly available and technology that is accessible only to law enforcement.[60] In *Kyllo v. United States*, the Court examined the warrantless use of an infrared thermal imaging device by law enforcement officers to gather sufficient evidence to support a warrant to search the defendant's home.[61] The government argued that the device merely told the police the temperature of the outside of the house (i.e. "off-the-wall" information) and did not provide "through-the-wall" information about the intimate details of the interior of the home,[62] and thus use of the imager did not constitute a search subject to the Fourth Amendment.[63] However, Justice Scalia wrote for the majority that since the imager was "a device that is not in general public use" that revealed

56. *Id.* at 708–10 (noting two instances in which the location of the beeper was lost by law enforcement after undetected movement from one location to another along public roads).

57. *See* United States v. Garcia, 474 F.3d 994, 996–97 (7th Cir. 2007) (finding that in light of *Knotts*, tracking a suspect's vehicle with an electronic tracking device as it moves on public roads is not a violation of the Fourth Amendment).

58. *See* United States v. Pineda-Moreno, 617 F.3d 1120, 1123 (9th Cir. 2010) (Kozinski, J., dissenting) (noting that those who store their vehicle in a garage are protected by a warrant requirement, while those who do not are subject to warrantless attachment of a tracking device to their vehicle).

59. *See infra* note 90 and accompanying text.

60. Kyllo v. United States, 533 U.S. 27 (2001).

61. *Id.*

62. *Id.* at 35.

63. *Id.*

information regarding the interior of the home that "would have been previously unknowable without physical intrusion," its use did constitute a search subject to the Fourth Amendment.[64] Scalia emphasized that it was important to craft a rule that did not leave the citizens of the United States "at the mercy of advancing technology . . . that could discern all human activity . . . ."[65]

This doctrine is unpredictable in that the rule articulated by the majority in *Kyllo* fails to achieve its essential purpose. Rather than providing a stable platform from which to view advancing surveillance technology, the rule actually leads to ever-increasing use of intrusive surveillance technology by the government as the technology enters mainstream use. For example, today warrantless use of cell phone and GPS tracking technology by law enforcement would not be considered a search under *Kyllo* because cell phones and GPS devices are widely available to the public. Therefore, *Kyllo* professes to protect the public from advancing technology but has the opposite effect. Any new technology that has been sufficiently taken up by the public becomes fair game for government surveillance.

Lastly, the Court has distinguished between surveillance technology that merely enhances a police officer's existing senses and technologies that provide information that would otherwise not be legally obtainable. In *Knotts*, for example, the Court held that the warrantless use of a tracking beeper on the defendant's car did not violate the Fourth Amendment because it merely augmented the officers' senses by making visual surveillance and tracking easier.[66] In *Kyllo*, on the other hand, the Court held that technology that revealed the heat information regarding the interior of the home was information that "would previously have been unknowable without physical intrusion."[67] Thus, the police's use of the thermal imaging device did constitute a search subject to the Fourth Amendment.[68] This doctrine is unpredictable because the courts have had a difficult time distinguishing between technology that merely enhances an officer's existing

64. *Id.* at 40.

65. *Id.* at 35–36.

66. United States v. Knotts, 460 U.S. 276, 282 (1983). The Court stated:

> The fact that the officers in this case relied not only on visual surveillance, but also on the use of the beeper to signal the presence of [the] automobile to the police receiver, does not alter the situation. Nothing in the Fourth Amendment prohibited the police from augmenting the sensory faculties bestowed upon them at birth with such enhancement as science and technology afforded them in this case.

Id.

67. *Kyllo*, 533 U.S. at 40.

68. *Id.*

senses and technology that provides otherwise unobtainable information. For example, in *Dow Chemical Co. v. United States*, the Court held that the use of high magnification precision aerial mapping photography without a warrant to determine Dow's power plant emissions did not violate the Fourth Amendment because it merely enhanced an officer's ability to see.[69] However, it is difficult to imagine how the information sought could have ever been otherwise legally obtained.

The unpredictability of Fourth Amendment case law results from the Court's struggle to respond to ever-changing interests in public safety and citizen privacy in the context of increasingly powerful technological means to obtain previously unobtainable information. Although some commentators have argued that the judicial branch is ill-suited to adjust to changing societal norms and advancing technology in a timely manner,[70] it is because of the Court's own rules in *Katz* and *Kyllo* that they must continue to weigh society's expectations of reasonableness against legitimate government interests in surveillance.

In addition to the Fourth Amendment, a system of laws enacted by Congress govern privacy in the United States. The principal statute in this area is the Electronic Communications Privacy Act (ECPA), enacted by Congress in 1986.[71] ECPA extended earlier statutory protections for electronic communications enacted under Title III of the Omnibus Crime Control and Safe Streets Act[72] and included two additional parts, the Stored Communications Act (SCA)[73] and the Pen Register Act,[74] to cover new advances in computers and communication.[75] However, ECPA specifically exempts data from tracking devices from the statutory protections provided under the Act in favor of the limited protections afforded under *Knotts* and *Karo* for information obtained from such devices because the data do not

69. 476 U.S. 227, 235–36 (1986).

70. Kerr, *supra* note 37, at 807–08 ("Legislatures do not offer a panacea, but they do offer significant institutional advantages over courts.").

71. Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1848.

72. Pub. L. No. 90-351, codified at 18 U.S.C. §§ 2510–2520 [hereinafter Title III].

73. 18 U.S.C. §§ 2701–2712 (2006).

74. 18 U.S.C. §§ 3121–3127 (2006).

75. ECPA is organized into three parts: (a) an updated Title III known as the Wiretap Act (WTA), providing strong protection for real time wire, oral, and electronic communications; (2) the Stored Communications Act (SCA), which provides weaker protection against government access to communications stored by a third party, and essentially codifies the Court's third party doctrine; and (3) the Pen Register Act, protecting pen register, envelope, and other non-content information voluntarily conveyed to third parties.

constitute an electronic communication.[76] The ECPA, and the SCA in particular, has been criticized by fourth amendment scholars as contrary to constitutional principles.[77] The ECPA intersects with the Fourth Amendment in complex ways because, regardless of the technologies at issue, all government searches must comply with the fundamental principles of the Fourth Amendment.[78] However, a full discussion of the ECPA is beyond the scope of this Note.

II. THE PERVASIVENESS OF CELL PHONE AND GPS TECHNOLOGIES AFFECTS THE BALANCE BETWEEN PRIVACY PROTECTION AND LAW ENFORCEMENT SURVEILLANCE

From the above review of technology surveillance law, one can see both the Supreme Court and the legislature's attempts to balance the privacy interests of individuals with the government's interest in legitimate law enforcement activity. With the development of new technologies such as cell phones and GPS that can also be used by law enforcement for surveillance purposes, it is important to reconsider whether the balance struck in existing law is still relevant. This Part examines the potential for cell phone and GPS technology to erode Fourth Amendment and statutory protection from warrantless surveillance. It reviews both technologies in the context of location surveillance and identifies ways in which the existing legal framework does not adequately address the potential for intrusive

76. 18 U.S.C. § 2510(12)(C) (" '[E]lectronic communication' . . . does not include . . . any communication from a tracking device"). Further, the protections under the SCA do not apply to GPS tracking cases because the information obtained about the first party (i.e. the suspect) is not willingly handed over to a third party.

77. For example, Daniel Solove has argued that provisions of United States Patriot Act that extend the ECPA and enable the government to access personal data without a warrant implicate First Amendment concerns due to the chilling effect this information gathering activity has on an individual's freedom of speech and association. Daniel Solove, *The First Amendment as Criminal Procedure*, 82 N.Y.U. L. REV. 112, 170 (2007). Other scholars have argued that the SCA is unconstitutional, as applied, because it affords government access to communications that society reasonably expects are private. *See, e.g.*, Orin Kerr, *Applying the Fourth Amendment to the Internet: A General Approach*, 62 STAN. L. REV. 1005, 1037–38 (2010); Alexander Scolnik, *Protections for Electronic Communications: The Stored Communications Act and The Fourth Amendment*, 78 FORDHAM L. REV. 349, 393 (2009).

78. *See, e.g.*, *In re* United States for an Order Directing Provider of Elec. Commun. Serv. to Disclose Records to the Gov't, 620 F.3d 304, 313 (3d Cir. 2010) (holding that, notwithstanding provisions of the SCA providing for a court order compelling a cellular service provider to hand over cellular site location information without a warrant, a magistrate judge may require a showing of probable cause sufficient to support a warrant if the Fourth Amendment is implicated).

government activity. In so doing, this Part also provides background for understanding why the District of Columbia Circuit's decision in *United States v. Maynard* reflects an important step in re-striking the appropriate balance between the government's need to gather evidence of crimes and the public's interest in individual privacy.

A. CELL PHONES AS UBIQUITOUS TRACKING DEVICES

There are over 292 million cell phone subscribers in the United States.[79] Indeed, many households use cell phones exclusively rather than the traditional landline.[80] As long as a cell phone is turned on, it will attempt to communicate with any nearby cell service provider sites[81] approximately eight times every minute in a process known as registration,[82] or more colloquially, "handshaking."[83] This electronic communication between the one or more nearby sites and the cell phone allows a cell phone service provider (CSP) or law enforcement agent to determine the approximate location of the cell phone and thus, the likely location of the person who currently possesses the device.[84] When a cell phone handshakes with a nearby site, or when a user

---

79. CTIA—THE WIRELESS ASS'N, *CTIA's Semi-Annual Wireless Industry Survey*, 5 (2010), http://files.ctia.org/pdf/CTIA_Survey_Midyear_2010_Graphics.pdf.

80. CTR. FOR DISEASE CONTROL, *Wireless Substitution: Early Release of Estimates From the Nat'l Health Interview Survey, July–Dec. 2009*, 1 (2010), http://www.cdc.gov/nchs/data/nhis/earlyrelease/wireless201005.pdf (finding that 24.55 percent of households use a cell phone and do not have a landline, and an additional 14.9 percent of households had a landline but used a cell phone for nearly all their calls); Ryan Randazzo, *Qwest Seeks Exemption on Rates*, ARIZ. CENTRAL, 1 (July 11, 2008), http://www.azcentral.com/business/articles/2008/07/10/20080710biz-qwest0711-ON.html ("[N]early 16% of people no longer use landline phone service and instead solely rely on cellphones.").

81. Traditionally, such sites are referred to as cellular "towers." However, with the increasing use of devices such as micro, pico, and femto cells, which are not necessarily deployed as towers, the term "towers" has become too narrow.

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

> This process, called 'registration,' occurs roughly every seven seconds when the cell phone is turned on; the user of the phone does not need to take any action, and is probably unaware that the phone is sending these signals. The only way to stop these signals is to turn the phone off. These location signals are sent on one band—the other two frequency bands that the phone uses are for sending and receiving voice and data.

Id.

83. *See, e.g.*, Michael Isikoff, *The Snitch in Your Pocket Law*, NEWSWEEK, Mar. 1, 2010, at 40, *available at* http://www.newsweek.com/2010/02/18/the-snitch-in-your-pocket.html (recounting an anecdote where law enforcement "agents were able to follow a Mexican drug-cartel truck carrying 2,200 kilograms of cocaine by watching in real time as the driver's cell phone 'shook hands' with each cell-phone tower it passed on the highway").

84. *Id.* It is unclear whether the information provided by the registration process is stored, or is only available in real-time, and different providers may treat this information

places or receives a call, or sends or receives data such as a text message, a voice mail, or a webpage, a CSP may obtain the phone's location information from the strength of the signal to one or more provider sites, the time difference of arrival of the signal between two or more sites, or the angle at which the signal arrives at one or more sites.[85] This location information derived from communication between the cell sites and the cell phone is known as cell site location information (CSLI or CSI).[86]

Some cell phones also have GPS devices already installed.[87] GPS devices obtain location data by measuring the distance from the unit to a set of dedicated GPS satellites.[88] GPS devices require reception of a satellite signal to operate; and unlike a cell phone, they only work when the devices have a line of sight to the sky.[89] Thus, they do not work indoors.[90] Although GPS devices themselves, in general, do not transmit their location to any third party, such as a CSP, many cell phones are equipped to, and do, transmit data

differently. Traditionally both the legislature and the courts have distinguished between stored or historical information and real-time information, considering the public to have a heightened expectation of privacy in the latter.

85. *See In re* United States for Order for Disclosure of Telecomm. Records, 405 F. Supp. 2d 435, 437 (S.D.N.Y. 2005). The court stated:

> Under prior orders issued in this District, the Government has been able to obtain a list of each call made by the subject cell phone, along with a date, start time and end time. With respect to the beginning or end of the call (and possibly sometimes in between), there is a listing of a three-digit number assigned to a cellphone tower or base station. At least one cellular provider will give, in addition to the number of the tower, a digit ('1,' '2' or '3') indicating a 120 degree 'face' of the tower towards which the cell phone is signaling.

Id.

86. *See, e.g.*, *In re* United States for an Order Directing Provider of Elec. Commun. Serv. to Disclose Records to the Gov't (*In re United States*), 620 F.3d 304 (3d Cir. 2010) (using term CSLI); *In re* Application of U.S. for an Order Authorizing the Release of Historical Cell-Site Info., 736 F. Supp. 2d 578 (E.D.N.Y. 2010) (using term CSI). CSLI may be categorized as either historical, in that it exists as a stored communication and is subject to the SCA, or real-time, in that the information is currently in transmission and subject to the stronger protections of the WTA.

87. Popular cell phones containing GPS devices include, for example, versions 2, 3, and 4 of the iPhone®, and all current Palm®, and Blackberry phones®.

88. Richard B. Langley, *In Simple Terms, How Does GPS Work?*, UNB: DEP'T OF GEODESY & GEOMATICS ENGINEERING (Feb. 16, 2008), http://gge.unb.ca/Resources/HowDoesGPSWork.html.

89. GARMIN LTD., http://www8.garmin.com/aboutGPS/ ("[GPS] signals travel by line of sight, meaning they will pass through clouds, glass and plastic but will not go through most solid objects.") (last visited Apr. 3, 2011).

90. SCI. AM., http://www.scientificamerican.com/article.cfm?id=indoor-positioning-system ("But [GPS] has its limits—most notably, roofs, walls and floors that shield satellite signals and keep them from locating GPS receivers indoors.") (last visited Apr. 3, 2011).

from the GPS device present in the phone to the CSP, unless the feature is specifically disabled by the user.[91]

B. GPS BASED TRACKING DEVICES ARE NOT AN UPDATED VERSION OF THE BEEPER IN *KNOTTS*

Warrantless GPS tracking of objects other than cell phones presents a different situation than cell phone tracking. Tracking via CSLI and cell phone GPS, as explained *supra* Section II.A, involves converting the widely used cell phone into a location-identification device by accessing non-public information held by third-party CSPs. GPS tracking, on the other hand, involves the use of a specialized vehicle-tracking devices generally only available to law enforcement. Typically, warrantless GPS tracking involves the attachment of such a device to a suspect's car or other belongings.[92] This requirement presents practical difficulties not present with cell phone tracking because it requires physical access to the item to be tracked and some maintenance, such as the replacement of batteries. Such tracking also presents the risk that the device might be inadvertently discovered by the suspect.[93] GPS tracking devices used by law enforcement agents vary in their technological sophistication. Newer devices are capable of transmitting the data gathered to a receiver or CSP so that once installed, the data can be obtained without physical access to the item being tracked.[94]

Although it might at first seem that this GPS information transmitted to a CSP involves the third-party doctrine and is no different from the GPS or

---

91. Andrew Brandt, *Soon, Your Cell Phone May Be Tracking You*, PC WORLD (Feb. 25. 2004, 1:00 AM), http://www.pcworld.com/article/114721/privacy_watch_soon_your_cell_phone_may_be_tracking_you.html ("[P]roviders . . . [insist] that any phone with a GPS chip in it lets you disable the tracking features (though the option is usually buried in the phone's settings menu) . . . [b]ut if you don't, your phone may reveal much more about you."). Additionally, many GPS-equipped cell phones provide access to mapping or direction-finding services such as Google Maps. In order for the mapping and direction-finding services to work, the phone's location must be identified by GPS and transmitted to the service provider; the resulting information is then used to determine the optimal route or determine which sections of map to transmit back for display to the user.

92. United States v. Maynard, 615 F.3d 544, 555 (D.C. Cir. 2010); State v. Jackson, 76 P.3d 217, 256 (Wash. 2003); *cf.* United States v. Pineda-Moreno, 591 F.3d 1212, 1213 (9th Cir. 2010).

93. Mina Kim, *FBI's GPS Tracking Raises Privacy Concerns*, NPR (Oct. 27, 2010), http://www.npr.org/templates/story/story.php?storyId=130833487 (detailing the story of United States citizen Yasir Afifi, whose mechanic discovered a GPS tracking device owned by the FBI during a routine oil change).

94. The GPS-205 from CES Wireless, for example, can be attached the underside of a vehicle by law enforcement agents wherein it will transmit its location every three seconds over a cellular phone network. *See* CES WIRELESS http://www.ceswireless.com/ (last visited Mar. 9, 2011).

CSLI data obtained from a suspect's cell phone, it is important to note that the data in this case is not being voluntarily handed over to the CSP by the suspect. In fact, the suspect has no access to or possessory interest in the data because the information is not transmitted from the suspect's device to the suspect's CSP; rather, it is transferred from the law enforcement agent's device to the law enforcement agent's CSP.

Similarly, the GPS devices currently used by law enforcement also differ markedly from the beeper devices[95] they are often compared to by the courts[96] because of the information they provide. Broadly speaking, it is true that both a beeper and a GPS device provide location information. However, the beepers used in *Knotts* and *Karo* were simple radio transmitters of limited range[97] that forced the agents tracking the device to stay in close physical proximity to the device.[98] In contrast, the functionality of a GPS device is essentially unlimited by any distance between device and agent. Further, the beeper device only provides low-resolution directional information, including the approximate angle between the receiver and the beeper and the approximate distance as judged by signal strength.[99] Precise location information is simply unavailable from such a beeper device.[100] These limitations severely restrict the functionality of a beeper device. For example, the court in *Karo* noted several instances in which the installed GPS device was moved in a manner undetected by the agents tracking the device.[101] In

95. *See* United States v. Karo, 468 U.S. 705, 718 (1984) (holding that a warrant is required to obtain information from a beeper device in a suspect's home); United States v. Knotts, 460 U.S. 276, 285 (1983) (holding that a warrant is not required to track a suspect traveling on a public road with a beeper device).

96. *Pineda-Moreno*, 591 F.3d at 1216 (holding that the ruling in *Knotts* regarding the warrantless use of beeper devices governed the warrantless use of GPS devices).

97. *See* Clifford S. Fishman, *Electronic Tracking Devices and the Fourth Amendment:* Knotts, Karo *and the Questions Still Unanswered*, 34 CATH. U. L. REV. 277, 282 n.7 (1985) ("In congested urban areas, interference with the reception of the beeper's signals may reduce its effective range to about two blocks.").

98. *Knotts*, 460 U.S. at 278 (1983) (describing how officers lost their beeper signal shortly after the suspect began taking evasive maneuvers); United States v. McIver, 186 F.3d 1119, 1123 (9th Cir. 1999) (describing the use of "an electronic transmitter that sends a weak signal or a 'beep' to an audio unit ('monitor') installed in the officer's vehicle. When the monitoring vehicle gets close to the transmitter, the signal received in the audio unit becomes stronger. The monitor also contains a 180 degree dial with a needle that points in the direction of the transmitter.").

99. *McIver*, 186 F.3d at 1123.

100. Tarik Jallad, *Old Answers to New Questions: GPS Surveillance and the Unwarranted Need For Warrants*, 11 N.C. J.L. & TECH. 351, 355 (2010) ("Accuracy and reliability, however, [are] not the beeper's *forte*.").

101. *Karo*, 468 U.S. at 708–09 (detailing undetected movement of the device from one suspect's house to another, and then from the second suspect's house to a storage locker).

contrast, a GPS tracking device may record and transmit its location with sub-meter accuracy and will never be out of range.

III. MANY COURTS HAVE BEEN UNABLE OR UNWILLING TO APPLY STRONG FOURTH AMENDMENT PROTECTION FROM CELL PHONE AND GPS TRACKING

A. *UNITED STATES V. GARCIA*

In *United States v. Garcia*, law enforcement agents, acting on an informant's tip, attached a GPS tracking unit to defendant Garcia's car while it was parked in a public area.[102] The police learned from the GPS tracking unit that the defendant was visiting a large tract of land, and a subsequent search of this land revealed evidence of the suspected drug manufacturing.[103] At trial, Magistrate Judge Crocker held that the police had a reasonable suspicion sufficient to support the lawful attachment of the GPS device.[104] The district court also held that even under the probable cause standard, police had sufficient basis to support the search without obtaining a warrant.[105]

On appeal to the Seventh Circuit, the defendant argued that because the police did not obtain a warrant supported by probable cause authorizing the installation of the GPS tracking device, the GPS evidence should have been suppressed at trial[106] because the attachment of the device to the undercarriage of the defendant's car was a seizure within the meaning of the Fourth Amendment.[107] The court found this reasoning "untenable," noting that the device in no way impeded any use or value of the vehicle.[108] The court also analyzed whether a search had been performed within the meaning of the Fourth Amendment and concluded that it had not.[109] The court held that the GPS tracking, unlike the use of a thermal imaging device in *Kyllo*, is

102. 474 F.3d 994, 995 (7th Cir. 2007).

103. *Id.*

104. United States v. Garcia, No. 05-CR-155-C, 2006 WL 1294578, at *6 (W.D. Wis. May 10, 2006) ("If it turns out that the government's actual burden of proof required a probable cause showing, then . . . the government met this burden.")

105. *Id.*

106. *Garcia*, 474 F.3d at 995.

107. *Id.* In this context, seizure does not mean actual taking by the government of a suspect's personal effects; rather, it is a constructive taking in which the value of a suspect's personal effects is diminished by government action.

108. *Id.*

109. *Id.* at 996–97 (confirming the finding in *Knotts* that "following a car on a public street, . . . is unequivocally not a search within the meaning of the [Fourth] Amendment.").

merely a substitute for a type of activity which is clearly not a search under the Fourth Amendment—namely, visually tracking a moving vehicle.[110]

The court concluded that while "wholesale" surveillance of "thousands of cars at random" using GPS tracking technology may present compelling Fourth and Fifth Amendment issues, the type of tracking employed in this case was not a Fourth Amendment violation because GPS tracking is not a search or a seizure.[111] Although the court emphasized that its holding does not apply to the type of wholesale surveillance that GPS tracking technology presumably enables,[112] as explained *supra* Part I, this ignores the warning in *Knotts* that the rule there that a person's travels on public roads are not private information should not be extended to cover continuous and prolonged electronic surveillance.[113]

B. *UNITED STATES V. MARQUEZ*

In *United States v. Marquez*, defendant Marquez sought to exclude information obtained when law enforcement agents continuously tracked defendant's vehicle from May 2007 to October 2007.[114] The Eighth Circuit held that *Knotts* controls GPS tracking of vehicles by law enforcement, finding that a person traveling via automobile on public streets has no reasonable expectation of privacy in his movements from one locale to another.[115] The court noted that "[c]onsequently, when police have reasonable suspicion that a particular vehicle is transporting drugs, a warrant is not required when, while the vehicle is parked in a public place, they [may] install a non-invasive GPS tracking device on it for a reasonable period of time."[116]

Echoing *Knotts*, the court then explained that its ruling does not apply to "wholesale" surveillance in which such devices are attached to thousands of random cars.[117] The court distinguished the instant case from such wholesale

110. *Id.* at 997 ("GPS tracking is on the same side of the divide with the surveillance cameras and the satellite imaging, and if what they do is not searching in Fourth Amendment terms, neither is GPS tracking.").

111. *Id.* at 998.

112. *Id.* ("It would be premature to rule that such a program of mass surveillance could not possibly raise a question under the Fourth Amendment.").

113. United States v. Knotts, 460 U.S. 276, 283–84 (1983) (holding that the Court's ruling that the use of electronic tracking devices is not a violation of the Fourth Amendment should not be construed as sanctioning "such dragnet-type" activities as "twenty-four hour surveillance").

114. 605 F.3d 604, 607 (8th Cir. 2010).

115. *Id.* at 609.

116. *Id.* at 610.

117. *Id.*

surveillance because the police "reasonably suspected that the vehicle was involved in interstate transport of drugs,"[118] which supported an action to install the GPS device and track the vehicle.

Unfortunately, the Eighth Circuit did not address the question of what constitutes a reasonable period of time, and ignored the Court's reservation in *Knotts* that their ruling did not sanction twenty-four-hour dragnet-type surveillance. This is unfortunate because, as explained *supra* Part I, when *Knotts* reserved the question of whether there would be a Fourth Amendment violation if law enforcement were to engage in "dragnet-type"[119] surveillance, the Court was not referring to "wholesale" and simultaneous surveillance of thousands of cars.[120] Rather, the Court, in *Knotts*, was referring precisely to the type of extended surveillance without judicial supervision at issue here, where *any* citizen's vehicle may be tracked without a warrant twenty-four hours a day, for months at a time.[121]

C. *UNITED STATES V. PINEDA-MORENO*

In *United States v. Pineda-Moreno*, the Ninth Circuit considered whether information obtained without a warrant via continuous surveillance using a GPS tracking device was a violation of defendant's Fourth Amendment rights.[122] In June of 2007, DEA agents noticed the defendant purchasing a large quantity of fertilizer from a retail store.[123] The law enforcement agents then followed the defendant to a trailer home that defendant was renting,[124] installed mobile tracking devices on the underside of the defendant's vehicle on seven different occasions, and monitored the vehicle's movements for four months.[125] In five instances, the defendant's Jeep was parked in a public

---

118. *Id.*

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

120. *Id.*

121. *Knotts*, 460 U.S. at 283–84. The Court stated:

> Respondent . . . expresses the generalized view that the result of the holding . . . would be that 'twenty-four hour surveillance of any citizen of this country will be possible, without judicial knowledge or supervision.' But the fact is that the 'reality hardly suggests abuse'; if such dragnet-type law enforcement practices as respondent envisions should eventually occur, there will be time enough then to determine whether different constitutional principles may be applicable.

Id. (internal citations omitted); *see supra* notes 49–56 and accompanying text.

122. 591 F.3d 1212 (9th Cir. 2010).

123. *Id.* at 1213.

124. *Id.*

125. *Id.* Although the mobile tracking devices are never identified by either the district or appellate court as GPS tracking devices, I am not aware of any other type of device which would have been capable of tracking the vehicle in the remote areas visited. Regardless, the

place.[126] In two other instances, the Jeep was parked in the defendant's driveway, a few feet from the side of his trailer.[127] The driveway was publicly accessible, lacking any fence, gate, or no trespassing signs,[128] and the devices were attached between four and five a.m.[129] When the mobile tracking device showed that the defendant was near a suspected marijuana plant site, agents followed the Jeep and arrested the defendant,[130] who was found with a large quantity of marijuana.[131] At trial, the defendant conditionally pled guilty to conspiracy to manufacture marijuana.[132]

On appeal, the defendant argued that by attaching tracking devices to his Jeep, agents invaded an area in which he possessed a reasonable expectation of privacy, thus violating the Fourth Amendment.[133] The Ninth Circuit held that defendant's expectation of privacy was not reasonable regardless of whether the device was attached while the vehicle was parked in defendant's driveway or in a public place.[134] The court held that installing a tracking device to the underside of defendant's Jeep between four and five a.m., while the vehicle was parked in the driveway adjacent to his house, did not violate his Fourth Amendment rights.[135] The court reasoned that the facts showed that no gate, fence, or trespassing signs had been placed by defendant to protect the driveway from access by the public.[136]

The court separately examined whether the continuous four months of tracking implicated Fourth Amendment concerns beyond those identified in *Knotts* and *United States v. McIver*, a case similar to *Knotts* from the Ninth Circuit.[137] The defendant, channeling the Supreme Court in *Kyllo*, argued that the agents' continuous monitoring of his vehicles location over a long period of time violated his Fourth Amendment rights because "such devices are not used by the public."[138] The defendant further argued that although *Knotts* holds that a person traveling in a vehicle on public roads has no reasonable

devices are functionally equivalent to GPS tracking devices for the purposes of this Note in that in no case did the defendant voluntarily relay his location information to a third party.

126. *Id.*
127. *Id.*
128. *Id.*
129. *Id.*
130. *Id.* at 1214.
131. *Id.*
132. *Id.*
133. *Id.*
134. *Id.* at 1215.
135. *Id.* (citing United States v. McIver, 186 F.3d 1119, 1126 (9th Cir. 1999)).
136. *Id.* at 1213
137. *Id.* at 1214; *McIver*, 186 F.3d 1119.
138. *Pineda-Moreno*, 591 F.3d at 1216.

expectation of privacy, *Knotts* does not control because *Kyllo* superceded the holding in *Knotts*, when the Court held it illegal for law enforcement to use surveillance technology that was not in public use to obtain private information without a warrant.[139] The court was not persuaded by this argument; it found that unlike *Kyllo*, where thermal imaging technology was used as a substitute for an activity that requires a warrant (i.e., a home search), the instant case, as in *Knotts*, regarded using tracking technology as a substitute for an activity that does not require a warrant (visual surveillance of a person's public travels).[140]

Subsequent to the Ninth Circuit's holding, the defendant filed a petition for an en banc rehearing of the case, which was denied.[141] Although the *Pineda-Moreno* decision and the denial of petition for en banc rehearing would suggest that, in the Ninth Circuit at least, warrantless GPS tracking is business as usual,[142] the dissent from denial of rehearing suggests that a number of justices have become uncomfortable with the pervasive tracking at issue here. Chief Judge Kozinski, with Judges Reinhardt, Wardlaw, Paez, and Berzon joining, dissented from the majority ruling denying the rehearing.[143] Their dissent focused on the alarming erosion of the scope of Fourth Amendment protection and the intrusiveness of new surveillance technologies used by law enforcement agents.[144] The dissent argued that the majority had created a system where the rich and powerful are protected from such devices by virtue of the fences they live behind and the security guards that patrol their neighborhoods.[145] In contrast, those citizens of more modest means who cannot store their vehicles in protected garages are left to

139. *Id.*

140. *Id.*

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

142. Other circuit courts that have ruled on the GPS tracking issue have found that continuous GPS tracking without a warrant is not a violation of the Fourth Amendment. *See* United States v. Marquez, 605 F.3d 604, 609 (8th Cir. 2010) (holding that under the controlling doctrine of *Knotts*, "a person traveling via automobile on public streets has no reasonable expectation of privacy in his movements from one locale to another"); United States v. Garcia, 474 F.3d 994, 996–97 (7th Cir. 2007) (holding that attachment of GPS tracking device to a vehicle without a warrant or notice is not a seizure cognizable under the Fourth Amendment, and under *Knotts*, GPS tracking of a vehicle's public travels is not a search under the Fourth Amendment).

143. *Pineda-Moreno*, 617 F.3d at 1121–26 (9th Cir. 2010) (Kozinski, J., dissenting).

144. *See, e.g., id.* at 1124 ("By holding that this kind of surveillance doesn't impair an individual's reasonable expectation of privacy, the panel hands the government the power to track the movements of every one of us, every day of our lives.").

145. *Id.* at 1123.

the mercy of any law enforcement agents who wish to attach tracking devices to their vehicles.[146]

The dissent distinguished *Knotts* from *Pineda-Moreno* by analogizing the beeper in *Knotts*, with its limited range, lack of data logging, and low locational resolution, to a set of binoculars used to aid in visual surveillance of a moving vehicle.[147] Judge Kozinski reasoned that unlike with the beeper in *Knotts* or with a set of binoculars, "a small law enforcement team can deploy a dozen, a hundred, a thousand [GPS] devices . . . with far less effort than was previously needed to follow a single vehicle."[148] The dissent further criticized the alternate interpretation of *Knotts* found in the Seventh, Eighth, and Ninth Circuit Court opinions about GPS tracking. Namely, the dissent explained that "*Knotts* expressly left open whether 'twenty-four hour surveillance of any citizen of this country' by means of 'dragnet-type law enforcement practices' violates the Fourth Amendment's guarantee of personal privacy."[149] Judge Kozinski concluded that

> most people in the United States would [not] agree with the panel that someone who leaves his car parked in the driveway outside the door of his home invites people to crawl under it and attach a device that will track the vehicle's every movement twenty-four hours a day and transmit that information to total strangers.[150]

D. THE D.C. CIRCUIT LIMITS INVASIVE ELECTRONIC GOVERNMENT SURVEILLANCE

The District of Columbia Circuit's recent decision in *United States v. Maynard*[151] reflects an important step in re-striking the appropriate balance between the public's interest in privacy and the government's interest in gathering evidence and crime control. It, along with the Ninth Circuit's dissent in *Pineda-Moreno* and the Third Circuit's decision in *In re United States for an Order Directing Provider of Electronic Commuication Service to Disclose Records*, suggests that there is a growing unease within the circuit courts with

146. *Id.*

147. *Id.* at 1124.

148. *Id.* at 1124. The dissent presents no allegation that such mass surveillance via GPS tracking device is actually occurring, but does suggest that such mass surveillance is occurring by law enforcement's use of cell phone tracking. *See id.* at 1125 ("At the government's request, the phone company will send out a signal to any cell phone connected to its network, and give the police its location. Last year, law enforcement agents pinged users of just one service provider—Sprint—over eight million times.").

149. *Id.* at 1126.

150. *Id.*

151. 615 F.3d 544 (D.C. Cir. 2010), *en banc denied*, United States v. Jones, 625 F.3d 766, (D.C. Cir. 2010), *cert. denied,* Maynard v. United States, 131 S. Ct. 671 (2010).

warrantless use by law enforcement officers of pervasive tracking technology.[152] Together, these cases suggest that the courts are finally beginning to understand the danger that pervasive government access to private information in the electronic age presents to our democratic society and are adjusting accordingly.[153]

In *Maynard v. United States*, the D.C. Circuit found that the defendant's Fourth Amendment rights were violated when the police, without a warrant, used a GPS device attached to his vehicle to track his movements continuously for a long period of time.[154] Appellants Jones and Maynard respectively owned and managed a nightclub in the District of Columbia.[155] In 2004, the police began investigating appellants for drug possession and trafficking, placed a GPS tracking device on Jones's Jeep, and tracked his movements continuously for four weeks.[156] The police thus obtained information that proved essential to the prosecution's case that Jones was involved in drug trafficking.[157]

On appeal, the court examined several claims brought by appellants Maynard and Jones for improper admission of evidence, including the

152. 620 F.3d 304, 313 (3d Cir. 2010) (finding that pervasive cell phone tracking data may implicate Fourth Amendment concerns and thus require a warrant supported by probable cause notwithstanding provisions of the ECPA, which the government purports compel the courts to issue a subpoena to compel upon request); *Pineda-Moreno*, 617 F.3d at 1121–26 (9th Cir. 2010) (Kozinski, J., dissenting).

153. *See* Daniel Solove, *The First Amendment as Criminal Procedure*, 82 N.Y.U. L. REV. 112, 121 (2007) ("Government probing can lessen the effectiveness of democratic participation by depriving speakers of anonymity, which can be essential for forthright expression. . . . Government information gathering can also discourage or subdue conversations."); Katherine Strandburg, *Freedom Of Association in a Networked World: First Amendment Regulation of Relational Surveillance*, 49 B.C. L. REV. 741, 794 ("Extensive government relational surveillance using network analysis data mining techniques poses a serious threat to liberty because of its potential to chill unpopular, yet legitimate, association, and also because of the chilling of legitimate association caused by possibly incorrect assessment of both legitimate and illegitimate associational membership."); Orin S. Kerr, *An Equilibrium-Adjustment Theory of the Fourth Amendment* (GWU Law School Public Law, Research Paper No. 524, 2011), *available at* http://ssrn.com/abstract=1748222 (presenting the theory that the Court adjusts the scope of Fourth Amendment protection as technology changes in order to maintain a "status quo level of protection").

154. 615 F.3d at 566–67.

155. *Id.* at 549.

156. *Id.* at 549–51 (citing Rakas v. Illinois, 439 U.S. 128, 148–49 (1978)) (holding that although the Jeep was registered to Jones's wife, Jones still had standing to object to admission of the evidence because Jones was the exclusive driver of the Jeep). The court stated that "whether defendant may challenge police action as search depends upon his legitimate expectation of privacy, not upon his legal relationship to the property searched." *Id.*

157. *Id.* at 567–68.

evidence obtained from a GPS tracking device.[158] The court affirmed all claims except those regarding the GPS evidence used against Jones.[159] Specifically, the D.C. Circuit analyzed whether the district court had erred in admitting the GPS evidence at trial, focusing on whether *Knotts* applied to continuous GPS surveillance in which case there was no search subject to Fourth Amendment protection and whether, under *Katz*, the information obtained was that which society reasonably expects to be private.[160]

Regarding the first issue, the court held that *Knotts* did not apply to the type of pervasive and continuous location monitoring presented by this case.[161] Instead, the D.C. Circuit found that *Knotts* distinguished between the limited information available to law enforcement via use of a beeper and the prolonged twenty-four-hour surveillance at issue in *Maynard*.[162] The court explained that the present issue, whether a warrant would be required in a case involving twenty-four hour surveillance, was explicitly reserved in *Knotts*.[163] The court further declared that other circuits that had interpreted *Knott's* reservation of whether "drag-net" type surveillance is a Fourth Amendment search to only refer to mass surveillance had misconstrued the *Knotts* opinion.[164]

Applying the *Katz* two-prong test, the court held that Jones's expectation of privacy was subjectively held and was one which society was prepared to recognize as reasonable.[165] Specifically, the court held that despite the fact that a person's individual trips in public view were necessarily public, the intimate picture of the subject's life obtained by continuous electronic monitoring was information that society was prepared to accept as reasonably protected from the prying eyes of the public.[166]

---

158. *Id.*

159. *Id.* at 555–68. This Note focuses on the court's analysis of whether evidence obtained via warrantless GPS tracking was admissible at trial.

160. *Id.* at 563–64.

161. *Id.* at 555–58 (citing United States v. Knotts, 460 U.S. 276 (1983)).

162. *Id.* at 556 (finding that "[t]he Court [in *Knotts*] explicitly distinguished between the limited information discovered by use of the beeper . . . and more comprehensive or sustained monitoring of the sort at issue in this case.").

163. *Id.* (holding that the Court specifically reserved the question [of] whether a warrant would be required in a case involving "twenty-four hour surveillance.").

164. *Id.* at 556–57 (citing United States v. Butts, 729 F.2d 1514, 1518 n.4 (1984)) ("[W]e pretermit any ruling on worst-case situations that may involve persistent, extended, or unlimited violations of a warrant's terms."); *see* People v. Weaver, 12 N.Y.3d 433, 440–44 (2009); Renee McDonald Hutchins, *Tied Up in Knotts? GPS Technology and the Fourth Amendment*, 55 UCLA L. REV. 409, 457 (2007).

165. *See* discussion *supra* Part I (explaining the *Katz* test); *Maynard*, 615 F.3d at 558–64.

166. *Maynard*, 615 F.3d at 563.

In applying the *Katz* test, the court emphasized that Jones had not given up any expectation of privacy by exposing this information either actually or constructively to the public.[167] The court reasoned that the whole of his movements during the monitoring period was not actually exposed to the public because, unlike one's movements during a single journey, the likelihood any person or group could observe all of those movements is zero.[168] The court distinguished continuous GPS monitoring from the visual surveillance that *Knotts* held was merely enhanced with a beeper device,[169] finding that a primitive beeper device or visual surveillance could not obtain the continuous and prolonged location information that a GPS tracking device provides.[170] The court referenced practical considerations that make continuous visual surveillance for long periods of time essentially impossible to perform to bolster this point.[171] Additionally, the D.C. Circuit reasoned that Jones did not constructively expose this information because the whole of his movements constituted a different kind of information than the individual movements it comprises.[172] As an example of how the whole of a person's location information is a different kind of information than the sum of his individual trips, the court cited a New York State court opinion holding that prolonged GPS tracking "yields . . . 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 avocational pursuits."[173] The court also noted that prolonged GPS tracking may reveal a person's "preferences, alignments, associations, personal ails and foibles,"[174] or a "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."[175] In other words, the totality of the information (TOI) obtained was greater than the sum of the individual pieces of information that were exposed to the public, and should therefore be subject to greater protection.[176]

---

167. *Id.* at 558–63.
168. *Id.* at 559–60.
169. United States v. Knotts, 460 U.S. 276, 282 (1983).
170. *Maynard*, 615 F.3d at 565.
171. *Id.* (citing testimony from a former Chief of the LAPD in W.H. Parker, *Surveillance by Wiretap or Dictograph: Threat or Protection?*, 42 CALIF. L. REV. 727, 734 (1954)).
172. *Id.* at 560–63.
173. *Id.* at 562 (quoting State v. Jackson, 76 P.3d 217, 224 (Wash. 2003)).
174. *Jackson*, 76 P.3d at 224.
175. *Maynard*, 615 F.3d at 562.
176. *Id.* at 558.

The D.C. Circuit further found that the method of continuous monitoring was at least as intrusive as other activities that the Supreme Court found to be a search under the Fourth Amendment such as a urine test,[177] electronic eavesdropping on private phone calls,[178] inspection of a traveler's luggage,[179] or use of a thermal imaging device to discover the temperature inside a home.[180] The court also noted that state statutes protecting against warrantless GPS monitoring of its citizens[181] support its interpretation that society reasonably expects citizens to be free from the prolonged twenty-four-hour surveillance enabled by GPS tracking.[182]

Although the D.C. Circuit's opinion outlined above rejects the trend in favor of allowing prolonged and continuous electronic location tracking of individuals without judicial supervision, it is not at all clear whether other courts and commentators will find the argument convincing. Indeed, several of the D.C. Circuit's own judges are not convinced, arguing two major points in their dissent for in denial of an en banc rehearing of the issue.

In dissent, Judge Santelle first argued that, as in the Seventh and Eighth Circuit court opinions on GPS tracking, *Knotts* controlled the decision.[183] Judge Santelle further noted that *Knotts* clearly states that a person's travels on public roads are public information, and that "[n]othing in the Fourth Amendment prohibited the police from augmenting the sensory faculties bestowed upon them at birth with such enhancement as science and technology afforded them in this case."[184] The dissent further argued that since appellant's reasonable expectation of privacy for any one of his public trips is zero, the sum of all his trips combined is still zero because "the sum of an infinite number of zero-value parts is also zero."[185] Secondly, the dissent argued that the majority's holding would make prolonged warrantless visual surveillance itself illegal because Judge Santelle "cannot discern any distinction between the supposed invasion by aggregation of data between

177. *Id.* at 563–64 (citing Skinner v. Ry. Labor Executives' Ass'n, 489 U.S. 602 (1989)).

178. Katz v. United States, 389 U.S. 347, 351–53 (1967).

179. Bond v. United States, 529 U.S. 334, 338 (2000).

180. Kyllo v. United States, 533 U.S. 27, 37 (2001).

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

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

183. United States v. Jones, 625 F.3d 766, 768 (D.C. Cir. 2010) (citing United States v. Knotts, 460 U.S. 276, 281–82 (1983)) (Santelle, J., dissenting).

184. *Id.*

185. *Id.* at 769.

the GPS-augmented surveillance and a purely visual surveillance of substantial length."[186]

Justice Kavanaugh, in a separate dissent, noted that neither the majority, nor Santelle's dissent, paid heed to appellant's alternative argument that placing the GPS tracking device on appellant's vehicle without a warrant was an illegal seizure under the Fourth Amendment.[187] Although unwilling to indicate how compelling he found this argument, Judge Kavanaugh did at least acknowledge that a colorable claim may have existed.[188] However, such a finding would still lead to a circuit split over warrantless GPS tracking because as discussed in Section III.A., *supra*, the Seventh Circuit has explicitly rejected this approach.[189]

IV. ANALYSIS

Today, the D.C. Circuit stands alone in holding that prolonged and continuous electronic surveillance necessarily implicates the Fourth Amendment.[190] However, the government's ability to use cell phone and GPS records to obtain location information about an individual, as well as the use of GPS devices to track an individual, shows that continuous surveillance is not only possible, but may provide intimate details about a citizen's life that could not otherwise be legally obtained, unlike the crude beeper device in *Knotts* that merely augmented visual surveillance. Thus, the existing statutory protections and case law are no longer adequate to address this continuous dragnet-type surveillance.

---

186. *Id. But see Maynard*, 615 F.3d at 564 (holding that the majority opinion in no way applies to prolonged visual surveillance).

187. *Jones*, 625 F.3d at 770 (Kavanaugh, J., dissenting).

188. *Id.*

189. United States v. Garcia, 474 F.3d 994, 996 (7th Cir. 2007) (holding that defendant's argument that attachment of a GPS tracking device was a seizure under the Fourth Amendment was "untenable").

190. *Maynard*, 615 F.3d at 566–67. The Third Circuit takes a smaller step in allowing, but not requiring, a magistrate judge reviewing an order to obtain CSLI to either demand a showing as to why there is probable cause sufficient to support a warrant or demand a showing as to why the warrant requirement is not applicable. *In re United States*, 620 F.3d 304, 313 (3d Cir. 2010). Essentially, the Third Circuit implicitly adopts a totality of the information theory by finding that an individual has not knowingly and purposefully shared the totality of the information contained in CSLI, i.e. a continuous log of his whereabouts, merely by keeping a cell phone on his person, and is therefore not subject to the third party doctrine. *Id.* at 317. The Seventh, Eighth, and Ninth Circuits in contrast have found that prolonged surveillance does not implicate the Fourth. *Garcia*, 474 F.3d 994, 995 (7th Cir. 2007); United States v. Marquez, 605 F.3d 604, 607 (8th Cir. 2010); United States v. Pineda-Moreno, 591 F.3d 1212, 1213 (9th Cir. 2010). The other circuit courts have yet to rule on this issue.

For example, Fourth Amendment jurisprudence strongly protects information about the intimate activities of a person's home. As the Court in *Silverman v. United States*,[191] *Karo*,[192] and then *Kyllo*[193] has made clear, officers are greatly restricted in the types of activities and technologies they can bring to bear in gathering information about activities in the home compared to gathering information from other locales. Such a distinction may have been logical and easily administered before technologies existed to peer through walls, but makes little sense today. Indeed, although the Court has made clear that thermal imaging cameras require a warrant to gather information about the interior of a home, our government contends, and many—but not all—courts have agreed, that CSLI does not implicate Fourth Amendment concerns[194] despite its increasing ability to provide information about the presence of an individual within a specific home, or even a specific room of a building.[195] This inconsistency illustrates how assumptions about how different technologies operate and what information they reveal often lead to bad law.[196] Further, as technology continues to advance, even correct

191. Silverman v. United States, 365 U.S. 505, 510–12 (1961) (finding that officers' use of a "spike mike" to penetrate the home and listen to conversations therein consituted a violation of the Fourth Amendment although the intrusion was minor).

192. United States v. Karo, 468 U.S. 705, 718 (1984).

193. United States v. Kyllo, 533 U.S. 27, 40 (2001) (holding that the use of a thermal imager without a warrant to gather evidence of activities in the home is a violation of the Fourth Amendment).

194. *In re* United States Orders pursuant to 18 U.S.C. 2703(d), 509 F. Supp. 2d 76, 80 (D. Mass. 2007); *In re* United States for Order for Disclosure of Telecomm. Records, 405 F. Supp. 2d 435, 449 (S.D.N.Y. 2005). *But see*, *In re United States*, 620 F.3d 304, 313 (3d Cir. 2010) (finding that the Fourth Amendment may be implicated by a request to obtain historical CSLI).

195. *In re United States*, 620 F.3d at 313. *But see 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 Comm. on the Judiciary House Reps., 107th Cong. 12–30 (June 24, 2010) (Statement of Professor Matt Blaze) (testifying that CSLI information is becoming increasingly accurate to the point of identifying a person's location to within an individual floor or room of a building due in part to the increasing density of cell sites).

196. As one example, it is commonly understood by the courts that the use of night vision goggles by the police to peer into a person's home without a warrant is perfectly reasonable and not a violation of the Fourth Amendment because the goggles merely augment the senses of an officer by amplifying ambient light. Some courts resort to the analogy that night vision goggles are like a high-tech flashlight. In contrast, it is understood that the use of a thermal imaging device by the police without a warrant would be a violation of the Fourth Amendment because it provides information that would otherwise be invisible to an officer. In other words, officers cannot normally see infrared emissions. Unfortunately, this distinction is simply unwarranted because night vision goggles both amplify ambient visible light and display near infrared emissions to the user that are otherwise invisible to the naked eye.

assumptions cited by judges and lawyers from earlier cases can be incorrect even a few months or years later. Rather than apply static rules to specific technologies, application of the D.C. Circuit's TOI doctrine to changing technology could help by providing a judicially administrable rule that looks beyond the technology to the information itself and examines whether that information is that which society is prepared to accept as private. Such an approach would seem to offer both flexibility and rigor to Fourth Amendment analysis because it adheres closely to Justice Harlan's rule in *Katz*.[197]

A TOI analysis should examine three factors: (1) the length of time during which the search was performed, (2) the type of information obtained, and (3) whether that information has been voluntarily conveyed to the public. Regarding the first factor, the longer a search occurs, the higher the likelihood that intimate details of a person's life are obtained. Additionally, a lengthy search strongly implies that officers had ample time to obtain a warrant. Regarding the second factor, the type of information obtained also suggests the degree of intrusiveness of the evidence-gathering activity. If the information obtained is merely a snapshot of a person's travels on public roads to and from public places, then it is unlikely to implicate the Fourth Amendment. However, for example, if the information obtained allows one to infer a person's acquaintances and religious preferences by virtue of the places visited, then it is likely to implicate the Fourth Amendment. Similarly, continuous GPS tracking may allow an officer to infer many details concerning the presence of persons or things within a suspect's home that would be unobtainable using visual surveillance or a beeper device. Such information would be properly excluded at trial under the TOI doctrine, just as it was excluded under *Karo*.[198] The third factor accounts for the Supreme Court's holding that if a person voluntarily hands over information to the public, it is no longer private information.[199]

Although the Court in *Kyllo* professed to craft a rule that could flexibly adapt to changing technology and societal expectations,[200] the result has been unsuccessful. For example, the rule in *Kyllo* for whether the use of a given

197. *See* Katz v. United States, 389 U.S. 347, 359–62 (1967) (Harlan, J., concurring).

198. United States v. Karo, 468 U.S. 705, 718 (1984).

199. *See Ex parte* Jackson, 96 U.S. 727, 733 (1878) (finding that the outside of a first class envelope was voluntarily conveyed to the public and thus may be viewed during evidence gathering activities by the government, whereas the content of the envelope was sealed against public view and thus protected by the Fourth Amendment).

200. Kyllo v. United States, 533 U.S. 27, 34 (2001) (purporting to adopt a rule that "assures preservation of that degree of privacy against government that existed when the Fourth Amendment was adopted").

technology by law enforcement requires a warrant is based on whether it is "in general public use."[201] Therefore, the rule becomes less protective as more technology enters the public realm. Today, thermal imaging cameras, like the one at issue in *Kyllo*, are readily available to the general public.[202] Has the ruling in *Kyllo* that the police may not use a thermal imaging camera to search a home therefore been superceded by advancing availability of technology to the general public?[203] Applying a TOI analysis as the D.C. Circuit has done for GPS tracking devices offers a judicially administrable way of analyzing whether the information sought is that which society would reasonably expect to be private information. Despite the availability of thermal imaging cameras from retailers like eBay and sports hunting outfitters, citizens do not expect that the thermal signatures of their homes are widely viewable by the public. Therefore, the doctrine does not change the outcome of *Karo*, it merely provides a more predictable rule that is stable in the face of changing technology.

Similarly, the Court in *Knotts* and *Karo* struggled to craft a rule that provided law enforcement with clear guidelines for when the use of an electronic tracking device without a warrant constituted a Fourth Amendment violation. However, the *Knotts* Court was careful to explicitly note that its rule, that a person's travel on public roads from one place to another is public information, was not meant to be applied to prolonged twenty-four-hour surveillance.[204] The TOI doctrine provides a judicially administrable way of reconciling the *Knotts* finding that the electronic tracking of a single trip is not a violation of the Fourth Amendment (because it is merely a substitute for visual surveillance), with the Court's concern that the rule does not address twenty-four-hour "dragnet-type"[205] surveillance. Although a person's travels on public streets from one place to another have been willingly conveyed to the public,[206] as the D.C. Circuit explains, the totality of the information obtained by continuous and prolonged monitoring provides a "mosaic"[207] picture that is beyond any information that has either

201. *Id.* at 34, 40.

202. For example, Ebay lists several varieties of thermal imaging cameras under the sporting goods category.

203. *See* Orin Kerr, *Can the Police Now Use Thermal Imaging Devices Without a Warrant? A Reexamination of Kyllo in Light of the Widespread Use of Infrared Temperature Sensors*, THE VOLOKH CONSPIRACY (Jan. 4, 2010, 12:33 PM), http://volokh.com/2010/01/04/can-the-police-now-use-thermal-imaging-devices-without-a-warrant-a-reexamination-of-kyllo-in-light-of-the-widespread-use-of-infrared-temperature-sensors/.

204. United States v. Knotts, 460 U.S. 276, 283–84 (1983).

205. *Id.* at 284.

206. *Id.* at 276.

207. United States v. Maynard, 615 F.3d 544, 562 (D.C. Cir. 2010).

been actually or constructively exposed to the public. The totality of the information provides a far too intimate picture of the private details of a person's life as compared to visual surveillance.[208] Therefore, applying the TOI doctrine to *Knotts* and *Karo* does not alter the outcome of those cases in that tracking of a single trip is not the type of intrusive surveillance of private details that implicates the Fourth Amendment, while gathering evidence about the contents of a person's home with an electronic device that would otherwise be unobtainable does implicate the Fourth Amendment.

Unlike *Knotts* and *Karo*, however, applying the TOI doctrine to the GPS tracking cases of the Seventh, Eighth, and Ninth Circuits would result in very different outcomes. In these cases, law enforcement officers tracked suspects continuously for months at a time, generating a detailed picture of the suspects' lives including "preferences, alignments, associations, personal ails and foibles."[209] Such information clearly implicates Fourth Amendment concerns under the TOI doctrine, and should only be obtained under the judicial supervision afforded by the warrant requirement.

Finally, the TOI may be applied to unknown or unimplemented technologies in predictable ways. For example, although our current airport screening techniques have alarmed some with their intrusiveness, they still do not provide a clear view of a passenger's person or things, as shown by the ease in which contraband still makes it through the screening procedure.[210] It is possible that advancing technology may continue to increase the intrusiveness of these screening techniques to the point where transportation safety personnel may be able to view even more intimate internal and external details of a person in an attempt to detect dangerous items. Regardless, under the TOI doctrine, the transitory and voluntary nature of the information gathering activity, combined with the type of information obtained (which does not provide an intimate and detailed mosaic picture of a person's life), would preclude a finding of Fourth Amendment implication.

In contrast, other technologies that do provide intimate details of a citizen's life may implicate the Fourth Amendment. For example, consider a future in which parents routinely implant their children with tracking devices

208. *Id.*

209. State v. Jackson, 76 P.3d 217, 224 (Wash. 2003).

210. Leon Kaufman & Joseph W. Carlson, *An Evaluation of Airport X-ray Backscatter Units Based on Image Characteristics*, 4 J. TRANSP. SEC. 73, 92–93 (2011) (detailing facile techniques for passing dangerous amounts of explosives and weapons through the newest and most powerful full body imagers used by airport screeners today); Philip Messing, *TSA Staff Jet Blew It, Boxcutters Taken on JFK Airliner*, NY POST (Mar. 2, 2011, 2:16 AM), http://www.nypost.com/p/news/local/queens/tsa_staff_jet_blew_it_Y7NcXScFd0oS2HNvkypthP#ixzz1IyPSIy4c.

that only work outdoors because the devices required a line of sight to a set of tracking satellites. Parents presumably would be interested in using such devices in order to keep tabs on their children, much like the way parents today provide their children with cellular phones. If the government were to seek access to such tracking device without a warrant, the Seventh, Eighth, and Ninth Circuits would presumably respond that, according to *Knotts*, a person's public travels from one place to another is public information, and the Fourth Amendment is not implicated. However, applying the TOI doctrine, it is clear that the prolonged tracking, the intimate details obtained, and the involuntary nature of the evidence gathering would suggest that a warrant is required. Such a result would seem to comport with Justice Harlan's view in *Katz* that the Fourth Amendment is meant to protect as private that which society is prepared to expect as reasonable.[211]

V. CONCLUSION

Interestingly, although the *Maynard* opinion rejects the Seventh, Eighth, and Ninth Circuit majorities' reasoning that GPS tracking does not require a warrant, the *Maynard* appellants' petition to the Supreme Court for a writ of certiorari was denied,[212] leaving an obvious and unresolved circuit split. Similarly, appellant's petition for en banc rehearing in front of the D.C. Circuit was also denied,[213] despite the suggestion of at least one prominent commentator that the ruling would be overturned.[214] Advocates for greater Fourth Amendment protection may find some comfort from this denial, but perhaps the Court is taking a wait-and-see approach to determine whether the D.C. Circuit opinion is the beginning of a trend.

Fourth Amendment scholar Orin Kerr has suggested that this wait-and-see approach by the judiciary is precisely the appropriate stance to take in the face of rapidly advancing technology that intrudes on the public's privacy interests.[215] Kerr posits that there is an equilibrium level of privacy that the Supreme Court, perhaps unknowingly, seeks to maintain.[216] As new technologies and surveillance techniques arise, government power expands

211. United States v. Katz, 389 U.S. 347, 361 (1967).

212. Maynard v. United States, 131 S. Ct. 671 (2010).

213. United States v. Jones, 625 F.3d 766 (D.C. Cir. 2010).

214. *See* 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/ ("I wonder if the [case] will [be] overturned en banc.").

215. Kerr, *supra* note 153, at 62–64.

216. *Id.* at 10.

and privacy interests become increasingly infringed. Later, as the Court begins to grasp with the impact of these technologies, the equilibrium is reestablished.

Unfortunately, this can take an inordinate amount of time because the judiciary is not expected to be, nor is it in practice, responsive to the will of the general public.[217] The Supreme Court is especially egregious in this regard. For example, although the Sixth Circuit has acknowledged that e-mail has become "the technological scion of tangible mail, and [that] it plays an indispensable part in the Information Age,"[218] some members of the Court are yet to master its use.[219] Kerr acknowledges that the judiciary can take an extremely long time to adjust Fourth Amendment jurisprudence,[220] but argues that this is a strength, because it allows the "nimble" legislature to enact statutory protections and provides the judiciary time to craft good law.[221] One wonders just how nimble the legislature can be considering the scant protections provided in the twenty-five-year-old ECPA, provisions of which have been called unconstitutional by scholars of Fourth Amendment law[222] and the Sixth Circuit.[223]

It is not just the public's interest in privacy that is at stake while the judiciary sits on the sidelines waiting to find a way back to some fundamental equilibrium. Law enforcement and the courts are also ill-served by policies that reduce the ability of agents to predict whether certain actions will be considered Fourth Amendment violations. The police need clear rules that

---

217. The democratically elected legislature is supposed to be more responsive to changes in society. *See* Orin S. Kerr, *The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution*, 102 MICH. L. REV. 801, 864–82 (2004) (arguing that legislatures have institutional advantages over courts in protecting privacy in changing technology). However, if this were true, then one might expect that the ECPA would more faithfully reflect the way contemporary society utilizes electronic communications.

218. United States v. Warshak, 631 F.3d 266, 286 (6th Cir. 2010).

219. John Hanna, *Sotomayor Touts Bipartisan Seating at Obama Speech*, MONTEREY COUNTY THE HERALD (last updated Jan. 28, 2011, 4:03 PM), http://www.monterey herald.com/news/ci_17219666?nclick_check=1 ("[S]everal unnamed justices haven't mastered e-mail.").

220. Kerr, *supra* note 153, at 64 (noting the thirty-nine year gap between *Olmstead* (allowing warrantless wiretapping) and *Katz* (holding that eavesdropping on telephone conversations without a warrant illegal)).

221. *Id.*

222. Orin Kerr, *Applying the Fourth Amendment to the Internet: A General Approach*, 62 STAN. L. REV. 1005, 1037–38 (2010); Alexander Scolnik, *Protections for Electronic Communications: The Stored Communications Act and The Fourth Amendment*, 78 FORDHAM L. REV. 349, 393 (2009).

223. *Warshak*, 631 F.3d at 288 ("[T]he SCA is unconstitutional.").

can guide actions on the street in order to do their job of protecting and serving the public effectively and legally.[224]

Rather than accept the damage that an unpredictable body of Fourth Amendment case law and outdated statutory framework causes in needless litigation, frustrated police activity, and intrusive government activity, the Court should recognize the core principal of privacy inherent in the Fourth Amendment and explicitly re-adopt the balancing test between privacy and public safety. Application of a TOI theory to evidence-gathering activity would help the police and the courts to recognize when certain activity requires a warrant. The standard is judicially administrable, utilizing an inquiry into whether the whole of the information sought is greater than could otherwise legally be obtained by the public, either actually or constructively. Ironically, this flexible approach, which can be applied in the context of a variety of surveillance technologies and fact patterns, is likely to provide more predictable outcomes for courts and law enforcement officers. By utilizing a TOI approach, courts can refocus on examining the core Fourth Amendment question of whether a person's fundamental privacy interest has been violated by government intrusion into an area unavailable to the public.

224. New York v. Belton, 453 U.S. 454, 459–60 (1981) ("When a person cannot know how a court will apply a settled principle to a recurring factual situation, that person cannot know the scope of his constitutional protection, nor can a policeman know the scope of his authority.").